Rethinking Initial HIPAA Efforts (HIPAA on the Job)

by Margret Amatayakul, RHIA, CHPS, FHIMSS

Many healthcare organizations met the compliance date of April 14, 2003, for HIPAA privacy by addressing the most visible features—implementing a notice of privacy practices, assigning an information privacy official (IPO), and conducting training sessions.

But a review of some organizations' actual practices and recent news stories reveals that knowledge and attention to detail may be superficial. This article will explore the current state of HIPAA privacy and security compliance, offer a risk-based approach to consolidating compliance efforts, and suggest an approach to achieving compliance through "piggybacking" on other IT initiatives.

Compliance Slipping for Some

Four months after the privacy rule compliance deadline, staff at one organization readily acknowledged that, despite the big push last year to shred paper containing protected health information (PHI), they had already become pretty lax. At another organization, the name of the IPO could not be identified by nearly 90 percent of clinical staff in a "post-HIPAA" compliance survey.

Most clinicians who were surveyed indicated they would "try" to ensure that a patient's friend who worked at the hospital would not learn about the patient's diagnosis, if requested. There was little recognition that the right to request a restriction was a HIPAA privacy right, that the organization had procedures on restrictions, and that there was significant risk involved in making decisions about restrictions. It is not that staff are inattentive or have blatant disregard for policy, but there was a lot to learn, and, in some cases, the rules seem contradictory to the industry's tendency toward a "caring" approach.

The HIMSS/Phoenix Health Systems' *Quarterly HIPAA Survey*, conducted during the first two weeks of July 2003, found that 77 percent of providers reported compliance with the HIPAA privacy rule, similar to the findings of its spring survey. Furthermore, of those providers professing to be compliant, 20 percent had not yet implemented a mechanism for compliance monitoring.

HIPAA Violations or Legal Matters?

The Office for Civil Rights (OCR) reported at the June meeting of the National Committee on Vital and Health Statistics that 637 privacy complaints had been received. Of these, 124 were closed without further investigation, primarily because they involved actions occurring prior to April 14. Accepted for investigation were 260 complaints, including several from employees reporting the organization for which they worked. By press time, the total number of complaints had risen to more than 1,800. CMS staff also indicated at a recent conference that they would accept anonymous complaints from employees.

Disconcerting evidence that HIPAA's initial efforts are not as strong as they could be is also revealed in several recent news stories. The August 28 *Houston Chronicle* reported the arrest of a hospital worker for theft of patient records for sale to a law firm. In May, the *Raleigh News and Observer* reported that a nursing assistant at a convalescent center was alleged to have ransacked a clinic's trash bins to obtain medical forms with identifying information to obtain credit cards and purchase personal items.

Some say these types of cases are legal matters, not HIPAA violations. A recent listserv posting reported that a hospital that contacted OCR about a former employee stealing records in retaliation for a termination was declined involvement. Looking at these cases, it appears that OCR is focusing on compliance issues and is not getting involved in enforcing the civil and criminal penalties of "wrongful disclosure" by a "person who knowingly and in violation of this part ... discloses individually identifiable

health information to another person."[1] And while the covered entities involved in these cases have fired workers and are cooperating with authorities, it is not clear how the wrongful disclosure penalties will be enforced.

Security Efforts Slow

In addition to some initial privacy efforts gone astray, security initiatives are also moving very slowly. In the HIMSS/Phoenix Survey, 55 percent of providers indicated they did not expect to be compliant with the security rule for more than a year. While the deadline is not until April 2005, security controls tend to require higher-priced and more complex solutions that should be budgeted now for implementation later.

Other organizations claim they have completed their security rule compliance activities by complying with the "mini-security rule" found in the privacy rule. Despite establishing fax and e-mail policies, instituting shredding, and repositioning workstations, many of these organizations have not documented a risk analysis nor have the means to describe residual risk to senior management. In many healthcare organizations, staff cannot identify a security incident. And many are lacking information system disaster recovery and technical access, audit, and authentication controls.

Risk-based Compliance

The HIPAA security rule requires a risk-based approach to compliance. It appears that some healthcare organizations may be extending the concept of risk-based compliance to all HIPAA requirements. If you are finding that some of the HIPAA buzz is wearing off in your organization, you may need a monitoring plan that establishes some minimum thresholds and benchmarks the industry to ensure that the landscape does not change and leave your initial efforts ineffective.

A good place to start is with a risk-based approach as required by the security rule:

For Privacy:

- Use your organization's overall risk management function to help manage privacy risk. A big "bucket" for "privacy," however, is insufficient to warn you that verification of identity and authority is not occurring, that authorizations for release of information are not being obtained for disclosures in certain areas, or that requests for restrictions are being attempted without follow-through. Work with your organization's risk management department to tease out privacy issues of which you should be aware.
- Coordinate risk management, corporate compliance, accreditation preparation, security incident reporting, and other quality improvement systems. Many organizations have so many places for reporting events, monitoring indicators, handling complaints, receiving questions, etc., that a small number of issues in any one area may not reveal that issue's true size.
- Find out what is most risky at your organization by walking around and talking with staff. Some other ways to take a "HIPAA pulse" are to pose a question in a newsletter, on an intranet site frequented by staff, or even when employees log on. This provides an "automatic survey" and heightens awareness. In the survey referenced above, the simple act of asking whether they shred paper with PHI reminded people that this was still important.
- Establish key indicators and mechanisms for monitoring that are based on your organization's highest risk areas, but also continue monitoring general information to determine the need to change your indicators. "HIPAA Risk Monitoring," below, offers some suggestions to document your risks and find ways to piggyback review of those on already-established monitoring systems.

HIPAA Risk Monitoring

Risk	Risk Indicator	Monitoring Mechanism
Identity theft	PHI in trash	Add to safety inspections
Unauthorized disclosure by imposters	Open campus	Use protective services to observe for badges
Accidental unauthorized disclosure	Complaints from recipients of misdirected PHI	Require quality improvement reviews by outsource company

For Security:

- The security rule requires that probability and criticality of potential risks to electronic PHI be used to decide what security measures are needed. Yet most organizations approach security controls from strictly a vulnerability perspective, with the goal being to "plug the gaps," whether there is true risk or not. Not only is this not meeting the HIPAA requirement for risk analysis, but it is most likely costing more. Use the security goals of confidentiality, integrity, and availability (CIA) to focus your risk analysis more on probability and criticality. See "Risk-based Security," below, for a sample template.
- Couple security risk analysis with privacy monitoring to strengthen the case for specific controls. For example, access controls need to support the privacy rule minimum necessary use standard. An intrusion detection system that may primarily protect against viruses that can harm integrity and shut down an information system can also help spot suspicious attempts at remote access.
- According to the security rule, an information security official (ISO) is supposed to be "responsible for the development and implementation of the policies and procedures required by [the security rule]."[2] A recent survey found that security direction was primarily driven by CIOs, with fewer than 10 percent having ISO involvement.[3] In part, the percentage is low because many organizations have not yet appointed an ISO. In other cases, the ISO is at the level of security analyst or manager and does not have sufficient authority to offer risk-based solutions. The ideal structure for the ISO is one where the position is equivalent to other compliance officers and there is a close enough relationship to the CIO so there is solid coordination with IT, yet sufficient independence, authority, and responsibility to focus on administrative and physical controls in addition to technical controls.

Risk-based Security

Gap	Threat	Probability	Criticality	Control
Shared network logon	Accountability for network logon unavailable	Very high	Little impact on confidentiality, integrity, availability	Increase senior management support for unique user ID for application logon
No emergency access procedures	Clinician access to PHI without treatment, payment, and operations relationship	Moderately high	Breach of confidentiality through unauthorized disclosure	Acquire break-the-glass technology
On-site storage	Disaster renders PHI unavailable	Moderately low	Unless hospital building is rendered unusable, data availability on site is critical	Redundant systems; back-up generator
Open ports in network	Introduction of malicious code	Moderate	Could alter the integrity of the data and impact availability	Intrusion detection system

Restarting a Stalled Effort

Some organizations are anxious to focus on patient safety and electronic health record (EHR) initiatives and are putting HIPAA matters aside. There are many privacy and security measures, however, that will strengthen your organization's ability to achieve these broader goals. If your HIPAA efforts are stalling, linking them to fresher initiatives may help.

For example, an EHR system wherein paper records are no longer maintained requires a fully redundant back-up system and strong disaster recovery system. If you are replacing dumb terminals with PCs, consider using thin clients or at least removing the ability to save to floppy disks and print except to specifically supervised printers to avoid theft by creating copies surreptitiously. Biometric authentication may also be a consideration in an EHR, especially if you can demonstrate that it will not only help overcome one hurdle in user logon (remember passwords), but will save money in the long run (through virtually no more password resets).

A computerized physician order entry system (CPOE) requires strong access controls and audit trails to ensure accountability of persons using the system. Personal digital assistants (PDAs) with handy formularies are great for reducing medication errors, but if they also serve to collect patient data, they are targets for mobile device security controls. Ideally these devices should be used only for data entry by requiring that data be stripped from cache. Many of these devices permit wireless access to your network.

You may also find that individuals with just a minimum of technical savvy, such as trainees who want to connect to school, researchers who want to review scientific papers online, or even salespersons who simply want to check their office voice mail, are setting up rogue access points on your wireless LAN. These LANs need constant vigilance to ensure these access points are removed. Remote patient monitoring also promotes patient safety and utilization management. Older forms may require e-mail or use of modem connectivity. A secure Web portal will not only provide greater security, but will be more user friendly.

Part of your organization's ongoing compliance monitoring strategy should be to regularly review the benefits achieved through IT applications. If benefits are not as strong as they could be, assess the privacy and security impact. New controls may ease privacy and security burdens and enhance the ability to acquire newer technology.

Rethinking Initial Efforts

You may be finding that some of your organization's HIPAA policies and procedures are being forgotten, were not very workable to begin with, or are being preempted. While hopefully you are not experiencing some of the risks being reported in the news today, your organization may be reluctant to press on HIPAA privacy or do much more with security.

But risks are increasingly prevalent. Hospitals are not immune; in fact, they are prime targets for crime such as identity theft because HIPAA emphasizes "only" PHI. We cannot forget the value that PHI may hold beyond taking care of our patients.

Notes

1. "Health Insurance Portability and Accountability Act of 1996." Public Law 104-191. August 21, 1996. Available at http://aspe.hhs.gov/admnsimp.

2. "Health Insurance Reform: Security Standards; Final Rule." 45 CFR parts 160, 162, and 164. *Federal Register* 68, no. 34 (February 20, 2003). Available at http://aspe.hhs.gov/admnsimp/.

3. Porter, William. "Fertile Fields." *Health Management Technology* (September 2002).

Margret Amatayakul *(margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.*

Article citation:
Amatayakul, Margret. "Rethinking Initial HIPAA Efforts (HIPAA on the Job series)." *Journal of AHIMA* 74, no.10 (November 2003): 16A-D.