Electronic Record, Electronic Security

by Mark Hagland

New technologies are enhancing the ability to protect patient information. But there's more to successful implementation than just what's inside the box.

Melanie Schattauer, RHIA, Jack Obert, and their colleagues at Mercy St. John's Health System in Springfield, MO, are about as far along as anyone is in preparing for the new HIPAA information security regulations. In the past couple of years, Schattauer, the organization's HIPAA and privacy officer, and Obert, the health system's technical information security officer, have performed a thorough security and privacy evaluation of the six-hospital, 1,000-bed organization. With a team of colleagues, they have been developing policies and procedures for both privacy and security. And they have been investing carefully and thoughtfully in an ever-increasing array of technologies that help protect patient information.

Nationwide, hospitals, medical groups, health systems, and health plans are moving forward as Mercy St. John's is, working to gear up for HIPAA's security regulations, and in the process investing in security-related technologies that authenticate users, safeguard computers, manage remote access, maintain audit trails, and create secure messaging networks. The capabilities of these technologies range widely, and they will continue to evolve, seemingly daily.

Beyond the safeguards of the new technologies, an additional, vital element is required, say security and privacy experts such as Schattauer and Obert—a plan. Thorough policies, with the involvement of knowledgeable HIM professionals, are essential for successful technology implementation.

The Technology Menu

Current technology offerings address a broad range of security issues, from restricting the tasks that can be performed on a particular workstation to securing remote access for health professionals working off site. Perhaps the hottest area of development right now is identity management, the authentication of users across a wide range of workstations and networks, sometimes even as they come into proximity of a workstation. Technologies fall into several broad categories, discussed below.

Audit Controls

One of the technologies that Mercy St. John's Schattauer finds very useful is audit control. Forensics tools such as these, she notes, are important in determining the sources of privacy, security, and compliance breaches.

Virtually every IT vendor with a clinical information system solution offers built-in capabilities for creating and maintaining audit trails on user access. Overall, the technology provides the ability to track who logs onto a workstation or network, when they sign on and off, the applications they use, and when they use them. However, the technology currently faces a key challenge in integrating audit controls across entire organizations. Security leaders in healthcare organizations say the industry is only at the beginning of a long path in this area.

Configuration Management

Other types of technologies allow for managing activity on a single workstation or across an entire network of workstations. Configuration management technologies can prevent the ability to download data and images from floppy disks and CD-ROMs onto a particular computer, for instance. Or the technology might be used to proactively manage, control, and monitor activity across all workstations, systems, and networks in an organization. Specific software solutions can be purchased to provide

configuration management; however, as an issue, configuration management involves the management of a broad range of activities and tasks.

Messaging Management

While very few patient care organizations are allowing clinicians to communicate directly with their patients using traditional e-mail, many are creating methods for clinician-patient messaging, as well as clinician-clinician messaging, using secure Intranets and other systems. A number of vendors offer programs that help manage these messaging systems. Many questions remain to be answered, however, including the extent to which and how such messages are integrated into the patient health record.

Remote Access Control

All patient care organizations must address the issues surrounding remote access control, though most are only in early stages in this area. Professionals at all stages of care are requesting remote access: physicians want to access lab data from their offices; home health nurses want to relay vital signs from patients' homes; HIM departments want to make it possible for coding professionals to work from off-site locations; and clinicians and others want to use wireless devices inside and outside the hospital setting.

Hospitals and health systems are creating wireless networks, either stand-alone networks that provide their own security and encryption features or virtual private networks, most often with multiple layers of security and encryption. Additionally, most healthcare organizations have Web sites or Intranets that transmit identifiable patient information in some form. Vendors are working with their client patient care organizations to ensure compliance with HIPAA security standards (especially strong authentication) while facilitating ease of use.

Mobile, wireless devices pose a growing challenge for security. Mercy St. John's allows mobile devices into the hospital system, but with requirements. "We've implemented a policy here that no wireless goes on the system without LEAP security —a mechanism that encrypts your wireless data as it's being transmitted from the handheld or mobile device to your local area network," says Obert. The encryption keys are rotated at predefined intervals. LEAP stands for Lightweight Extensible Authentication Protocol security, which has been developed as a proprietary protocol by Cisco Systems. The technology is being matched in capability by some emerging nonproprietary versions, including Extensible Authentication Protocol-Transport Layer Security.

Regardless of the specific software solution, Schattauer, Obert, and their colleagues are actively using technology to balance the need for strong and reliable security—especially of personal health information—with user demands for access and ease of use. "System-wise," Schattauer says, "remote access is probably a bigger issue for us right now than messaging is. Everybody here wants access and to be able to work from home or on a business trip or on vacation; and on a practical level, we want them to have access."

But as the demand for remote access has increased, more than technology has changed. Security consciousness has grown, too. "People in our organization and other patient care organizations have gotten more policy- and procedure-savvy," says Schattauer. "They're more cautious about whom they give remote access to."

ID Management

Arguably the issue of most immediate interest in security-related technology is identity management—the entire process surrounding the identification and validation of individuals accessing information systems, workstations, devices, and networks, and the ongoing authentication, tracking, and archiving of their use.

Until recently, most healthcare information systems were limited to identity badges and either simple username and password systems or systems that combined these with swipe cards or key-fob access devices. Some facilities have made a leap to high-tech biometric devices that identify users by fingerprint or retinal scan. Most industry experts, however, see a limited potential for biometrics in clinical care environments, given such practical problems as the use of latex gloves by clinicians and the expense of installing and maintaining the systems.

The leading edge in identification management is a proximity badge that carries detailed information about the individual and can open or shut down workstations from a walking distance or in a timed fashion. The most advanced of these applications transfer the validated user profile to other systems in the network.

"The key to identity management," says John Stanley, practice director for technology consulting at First Consulting Group, "is a strong authentication approach, which is a particular HIPAA requirement and regulation—that all users will be independently authenticated to the information systems environment." That authentication stage is where many technologies are emerging, says Stanley, most notably proximity technology, smart cards, and locating technology (which uses global positioning in some cases).

Stanley urges HIM professionals, especially those involved in the vendor selection process, to understand the two critical factors in the success of identity management systems. The first is smooth integration into the network and authentication environment, allowing users to log in efficiently and without manual keying. Complicated and time-consuming login or authentication is a major source of clinician and staff resistance, Stanley notes. The second critical factor is performance, particularly speed. A system that doesn't respond in "sub-two-seconds," says Stanley, won't be accepted.

Balancing speed of access, security, and a third element—reliability—is a challenge vendors will have to successfully address, says John Gildersleeve, CHPS, chief privacy officer at Geisinger Health System, an integrated health system that serves more than a million people in southeast Pennsylvania. Gildersleeve also points to identity badges that open and close workstations as a hot technology and says his organization is considering their use. He cites ease of use as a major benefit. But he points to a significant concern: if the physical technology fails, if there is an emergency, "how do you get into a workstation?"

Laying the Groundwork with Policy

More important than choosing one particular technology over another, Gildersleeve emphasizes, is laying the proper policy groundwork for successful implementation of security technology. "The real key," he says, "is that once you're in the system as a user, what administrative controls are in place?" In other words, systemwide policies and procedural controls must anticipate the technology. "There's nothing sexy about this," Gildersleeve admits, but he stresses that whatever solutions an organization chooses must flow from administrative access through to physical control.

Schattauer of Mercy St. John's agrees. "You can find the technologies," she says, "but you have to write the policy before you roll these things out." She expects policy issues to be especially challenging for wireless and mobile technologies because remote coders and transcriptionists will include contract employees. Schattauer advises organizations to have a contract in place that specifies how contract employees use wireless and mobile tools and how they will use the personal health information. Such contracts and policies should be in place before technology is launched. Schattauer and her colleagues have been working on role-based access for more than four years, she notes, and every patient care organization will face similar complexities.

Cheryl Martin, RHIA, MA, CIO of Tuomey Health Care System, in Sumter, SC, also stresses that policy must precede technology. There are many excellent security technology solutions out there, she says, but as patient care organizations shop for them, they must also create the policy and procedure infrastructures that will guide their use.

Martin emphasizes the need to undo years of haphazard practices in granting individual access. "For example, you'll get a call saying, 'Susie needs access exactly as Mary has,' but Mary may have transferred departments four times and not lost her earlier access." Martin and her colleagues at the 266-bed facility have spent a number of months developing access policies and protocols. "We bit the bullet and did up the whole matrix by job description," she explains.

The Role for HIM Professionals

If it seems that in the realm of information security all technology solutions ultimately loop back to people issues, well, that's exactly what they do, say Schattauer, Obert, Stanley, Gildersleeve, and Martin.

HIM experts, CIOs, information systems (IS) leaders, and consultants agree that HIM professionals should learn all they can about security technologies now. Vendor selection processes, implementation efforts, rollouts, and the ongoing, day-to-day activities of working with security-related technology will require HIM expertise and perspective. Getting closer to the IS

people in your organization is essential also. The organizations in which HIM professionals become most involved with the appropriate IS staff find the best technology solutions and experience the best implementations.

Take, for example, configuration management, says FCG's Stanley. One of the big decisions most providers must consider is the tradeoff between configuration control and user flexibility on a given device. Stanley has worked with FCG in hundreds of environments and says that everyone has a slightly different take on the matter. HIM professionals who are deeply involved in sorting out such issues, he says, will find themselves rewarded when their organizations end up with systems and implementations that meet everyone's information security goals and correctly balance security with user needs, according to their organizations' philosophies.

Ultimately, all technology issues rebound back to day-to-day management issues for HIM professionals, notes Joan Hicks, MS, RHIA, director of information services at UAB Health Services Foundation in Birmingham, AL. Hicks, who is deeply involved in preparing security vulnerability testing with UAB's main vendors, says, "We manage all the security incidents in our department—suspected intrusions, breaches of confidentiality, viruses—and 99 percent of the time it's a people issue." Hicks stresses strongly the need for HIM professionals to educate themselves as much as possible and get involved with their information systems colleagues in moving the information security ball forward together as a team.

"HIM professionals need to be able to have a relationship with the information security department, because they're not going to be able to learn everything themselves, that's not their role, and they won't have time for that," Mercy St. John's Schattauer concludes. "They'll need to come to an agreement about what each person's role is—the people in information security, in HIM—and come to a consensus about all this to protect personal health information." By working together, she emphasizes, it can be done.

Identifying the Challenges of Identification Technology

One of the hottest areas of security-related technology is ID management, the identification and validation of individual users. Vendors are moving ahead aggressively to address a number of key challenges, and new solutions and programs come onto the market every month. Among the questions vendors are trying to answer:

- How can a patient care organization minimize the number of user names and passwords clinicians and staff need to employ in their day-to-day work?
- How can programs be developed that will integrate the various products already being used in different departments and areas?
- How can those responsible for the security of information systems and patient health information balance the need to protect PHI from unauthorized access while facilitating and enabling the most streamlined and clinician-friendly patient care?
- What is affordable and possible?

***Mark Hagland** (MHagland@aol.com) is a Chicago-based healthcare journalist.*

Article citation:
Hagland, Mark. "Electronic Record, Electronic Security." *Journal of AHIMA* 75, no.2 (February 2004): 18-22.