Information Security: It Takes a Community

Save to myBoK

by Beth Hjort, RHIA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) reinforces what HIM professionals have known for a long time: security training is a prudent and valuable mission for an organization to support. Besides the obvious need for compliance with this new federal mandate, it's a chance to enlist or renew the support of the whole healthcare team for optimal ongoing operations and risk management.

Although at press time, HIPAA's final rule for the security regulations had not been released, the security training requirement isn't like to change dramatically.

HIPAA puts a finer point on an age-old obligation that conscientious organizations would have faced even without written regulations as we work to handle all patient information consistently. Further, HIPAA demands that we make this a practice for everyone in our extended organizational community. Although it currently only governs electronic information, if your organization has made the decision to handle all information with the same integrity, this is the time to relay or reiterate that philosophy. Each individual must recognize the difference he/she can make by applying information security requirements to every decision.

According to Dan Barron, information systems director for AHIMA, "The environment dictates the security policy." In healthcare, security is a critical area of integrity that's getting harder to control. "You can have the best in information technology (IT), but if the users lack knowledge and therefore, responsiveness, an organization operates at a serious disadvantage in protecting itself," Barron says. It takes an organizational community working together to address the integrity of patient information privacy.

Many organizations are well on their way to satisfying the HIPAA training regulations as they have adhered to the Hippocratic Oath, the American Hospital Association's Patient Bill of Rights, AHIMA's Code of Ethics, Joint Commission standards, state laws, case law, the Privacy Act of 1974, the Freedom of Information Act, and federal regulations governing confidentiality and alcohol and drug abuse-related patient records. And if we look past the preparation, system, and budget challenges and the deadline burden, we recognize that the government is urging us one step closer to the place we have been working to reach all along: protecting and maintaining the consumer population we serve, managing our risk, and tightening our control over privacy regulations that we have been operationg under for decades.

Delivering the Security Message

An information security training outreach effort must include all employees in all of your organizational entities, including those working at home. The regulation pertains to all staff (executives, board of directors, physicians, employees, and volunteers) who use or may possibly see confidential patient information that is currently or ever was in electronic form.

The message of seriousness should run through every aspect of training and subsequent updates and reminders. If your marching orders for developing a training plan didn't come from upper management, enlist high-level support before formalizing your program. Because the ultimate incentive for staying out of jail rests with the CEO, you may want to hold separate security training for the executive level and board of directors prior to expanding or rolling out your program. Leadership will set an internal example, and they are likely to be designing business partner agreements and commitments for information sharing that must also be compliant.

HIM leaders and information security officers should work closely with their information system (IS) departments. IS departments would be expected to have detailed technology security policies already in place, so abiding by this HIPAA

directive that enhances staff understanding will make their jobs much easier. By combining these with the administrative policies, you will have a significant piece of your awareness training outline.

For full compliance with the training expectations in any setting, five components would be integrated into security education: awareness training, periodic security reminders, virus protection education, monitoring login success/failure and discrepancy reporting, and password management.

Awareness Training

This effort will give participants knowledge of security policies and procedures and the importance of adherence. Customization of your presentation should include the input of HIM, risk management, quality management, human resources, IS, and any other department or employee working closely with security concerns. In addition to gaining knowledge, employees must understand the reasons for security. Explain the elements that apply to your organization:

- the **administrative directive** for adherence
- laws: give staff a broad understanding of the legislation governing healthcare responsibility for the policies your organization is using or has newly developed
- **scope:** explain who is involved and how far security training extends. Explain that new staff receive the same training through HR's orientation program before they can begin work. Tell them if the same principles apply to physicians, non-physicians, contractual employees, and those who work in satellite units or at home
- **extent:** what mediums, departments, or technologies do you have that deserve special mention?
- **benefit:** explain the benefit to staff personally as healthcare consumers. Inform them whether your organization allows staff to request audit trails of access to their own information
- **responsibility:** tell staff to be the eyes and ears of the organization. Tell them how they can help by knowing the policies, how to report a known or suspected breach, and how to err on the side of caution. Their astuteness may help to bring about development of a policy that didn't exist before
- **policies and procedures:** explain your organization's policies and procedures and where they can be easily accessed. Further, discuss how individual department nuances will be addressed as well as how the mandated complaint line works in your organization
- **ramifications:** explain the implications and penalties of security breaches, both to the organization and to the individual, including law suits, fines, imprisonment, loss of job, and loss of medical staff privileges. Note the loss of time that translates into financial loss. Include real-life examples that would demonstrate the intention of penalty enforcement or measure cost
- **overseers:** tell staff about the information security officer working full-time to address this function or the coordinator of the security effort in your organization. Tell them about policy-setting or decision-making bodies, such as the information security committee and the incident response team that investigates known or suspected breaches. Explain how these tie into the HR disciplinary process
- **ensuring adherence:** tell staff what the organization is doing to measure compliance. Give examples of back-end security audits and what they can show. Tell them if you have e-mail screening software that monitors what information is coming into and leaving your organization

Periodic Security Reminders

The need for security awareness continues after initial training is complete. Let existing technology and communication networks help you, such as reminders and updates in regular department meetings, newsletters or online education via

application service providers.

Sign-on security statements can also serve as ongoing security reminders. These messages are displayed every time a user is about to access confidential patient information. Change the visuals (screen color, display pattern, and wording) periodically to recapture the reader's attention. A sign-on statement could be "Be aware that the patient information you are about to view is highly confidential. It is protected by law and organizational policy from redisclosure. Consequences of unauthorized use may be punishable by civil or criminal penalties and disciplinary action up to and including job termination."

As a future provision, set up your security program so that it changes and grows along with your organization. Be sure organizational leaders know to include this important aspect so that new twists brought on by added entities, programs, services, or systems are communicated in a timely manner.

Virus Protection

"All viruses should be treated alike. We don't know initially whether their intent is comically trivial or maliciously devastating," Barron says. "Virus protection education would start with understanding what viruses are and what they can do."

In your organization, teach staff about how viruses are spread, how to recognize symptoms, best practices to follow when suspecting or experiencing a virus, the software that IS already uses to minimize virus effects, and how they can help to outsmart a potential infection. Be clear on the evolving intelligence of viruses and software limitations when new strains are released.

Make sure staff understand that operations can be brought to an abrupt halt, affecting patient care, support functions, and introducing organizational risk and lost time, representing a huge financial loss. Staff need to know that their role in interrupting a virus before it escapes from an individual computer to a network is critical.

"The best defense against virus attacks is to exercise common sense and caution when opening e-mail," Barron says. The most common manner in which virus programs are executed are through e-mail attachments. Therefore, Barron says, "beware of any e-mail messages from unfamiliar senders."

Login Success/Failure

Employee awareness of IS departments' security policies and technologies can help to detect deviation from normal access patterns. In addition to access levels, users can also be granted login privileges according to the number of tries, time of day, and machine and applications used. Let your IS staff detail what alerts a user would experience if attempts to work outside of these parameters are detected.

At login, if an employee is denied access due to "maximum number of logins exceeded" and he or she just arrived, it may mean that someone was attempting to gain access with his or her user name. Similarly, if an employee notices something unfamiliar on the screen and there was no notification by IS of changes, it would be prudent to report the circumstances. If files are missing, have been renamed, or if the visuals are different, make sure the staff knows how to detect and follow up on these concerns.

Password Management

Explain to staff why password management strategies-such as systems that force periodic password changes-are necessary. Employees should also be instructed not to post their passwords. If your organization uses biometric identifier keys such as fingerprints or retina scans, explain why their uniqueness precludes duplication. Explain your policies for logging out when leaving the work area or how your software works to automatically log out a user. Further, explain the added protection of using a minimum-length password containing both numbers and letters against password-cracking software.

Proof of Your Efforts

Although each of these labors have benefits of their own, be able to prove that the training occurred in case you are audited. Keep attendance logs and agendas or content documentation from training sessions. If you have used network or online

training options, ensure you can produce printouts validating employee participation. If you use department meetings, the minutes should record those in attendance. If broadcast e-mail is used for communiqués, update distribution lists regularly and form policies to reflect that. Retain copies of all pertinent materials. Some organizations choose to validate new employee training by retaining signed statements in employee files demonstrating attendance and understanding of security expectations in addition to annual confidentiality statements.

Barron offers a final guideline: "Teach all users to err on the side of over-communication. Something seemingly minute to you as an end user might be a significant discovery in maintaining trouble-free information systems management."

Resources

Abdelhak, Mervat et al. *Health Information: Management of a Strategic Resource*. Philadelphia: WB Saunders Company, 1996.

Brandt, Mary. "Information Security-An Overview." *Journal of AHIMA 67*, no. 6 (1996): insert after page 36.

Czirr, Karen. "Three Steps to Increasing Employee Information Security Awareness." *Journal of AHIMA 71,* no. 7 (2000): 30.

Federal Register 63, no. 155, August 12, 1998; p. 73187. Available at www.access.gpo.gov/su_docs/fedreg/ a980812c.html.

Sobel, David. "Essentials of Policy Enforcement." *In Confidence 7*, no. 2 (2000).

Acknowledgments

Dan Barron
Michelle Dougherty, RHIA
Harry Rhodes, MBA, RHIA
David Sobel

Beth Hjort *is an AHIMA practice manager. She can be reached at beth.hjort@ahima.org.*

Article citation:
Hjort, Beth. "Information Security: It Takes a Community." *Journal of AHIMA* 72, no.1 (2001): 67-69.
