HIPAA Security: Don't Disband the Committee Just Yet

Save to myBoK

by Stephen C. Brown, CISSP, ISSMP

By now, every healthcare organization has faced the initial security compliance responsibilities associated with HIPAA. However, the compliance road has not yet been fully traveled. The nature of the rule makes compliance a recursive effort of reassessment, continual auditing, regular education, and technology upgrades. Achieving compliance and maintaining compliance are two completely different things.

In order to maintain compliance with the HIPAA security rule, information security diligence needs to evolve from a project to an everyday operation. As of April 21, audit logs must not only be collected, but reviewed as well. Access rights must not only be properly assigned, but also periodically validated. A server that is patched and hardened today may be critically vulnerable tomorrow. Data security is a moving target and so is HIPAA compliance.

Changing the Security Mindset

Don’t let the HIPAA security committee disband once the initial compliance date passes. Its oversight will be needed to transform the compliance initiative into a regular information security management program using a standards-based approach to information protection.

Following an industry-accepted standard allows for continual measurement against current security practices by internal sources and trusted third-party auditors. The global ISO 17799 standard is a generally accepted approach to HIPAA security compliance. The National Institute of Standards and Technology also provides resources for developing a security management and HIPAA compliance program. The security committee should work with IT staff and trusted external resources to identify and apply an appropriate standard.

HIPAA Compliance Health Checks

The HIPAA evaluation standard requires healthcare organizations continually monitor changes in business processes, technology, and vulnerability to assess and manage risk. The best method for maintaining compliance is to conduct regular third-party assessments, which provide an impartial view of security operations. Third parties provide an unbiased view of an organization’s security and HIPAA compliance. In addition, professional assessment firms act as trusted advisers by bringing expertise and knowledge gained from working with peer organizations as well as companies outside of the healthcare industry.

Organizations contracting for a third-party information security assessment should keep several things in mind.

The company should have experience working in the healthcare market. Assessment reports should include the organization’s compliance gaps as well as accepted healthcare industry recommendations to close those gaps.

The firm should be able to demonstrate the technical capability to identify threats and vulnerabilities at the network, server, and application layers. Technical assessments should be conducted from both internal and external perspectives to identify known vulnerabilities and configuration errors. Corrective actions should be included for every identified issue.

Conducting an information security remediation effort can be resource intensive. **The contractor should be capable of supporting the organization in a remedial effort,** which could include technology implementation, policy development, and even staff augmentation.

The company should be capable of supporting the organization in a trusted role over time. This allows for a partnership with an outside resource that understands the specific needs of a healthcare organization and can be called upon to quickly support the organization when necessary.

Technology and Compliance: Moving Targets

A multilayered defense is the only suitable method to protect against the myriad threats that face healthcare organizations today. In order to continually protect patient health information, new security technology must be incorporated at every level of the electronic infrastructure. This includes protection at the desktop, server, and network levels. Just one example of a common problem facing hospitals is providing protection for remote physician offices with connections into the core infrastructure. Physicians' offices can create a critical security weakness in any healthcare organization's perimeter, and a well-configured firewall at a hospital's Internet gateway will do little to protect against a trusted connection to a doctor's office.

Fortunately, new technologies have been developed that place perimeter security devices within the scale and budget constraints of physicians' practices. Newly developed integrated security appliances provide gateway protection, intrusion prevention, and anti-virus, anti-spam, and routing capabilities. They also work in tandem with host protection technologies to provide affordable layered security for remote offices that are easily managed by a central console or even a third party.

One-time Security Awareness Training Is Only Effective Once

People are usually the weakest link in the information security chain. The best-written policies and procedures are only effective when followed. Firewalls may help keep intruders out of a network, but they will not stop an uninformed employee from opening unsafe e-mail attachments and introducing a virus into the network. Swipe cards cannot keep clinical staff from leaving written patient records in plain view. Security professionals understand that there is a direct correlation between user training and the number of passwords written on sticky notes hanging from monitors. The only way to maintain newly introduced security controls is to constantly reaffirm their importance to all staff.

Consistently delivering security awareness training is critical to ongoing compliance. A one-time training effort to achieve compliance by the April deadline will lose its effect over time. The challenge organizations face is how to deliver this training without devoting full-time instructors to in-services. The best approach is to develop an automated training program. Computer-based training can be delivered to anyone who has access to a workstation and, if properly developed, should require only minimal user support. This training should be designed to teach everyone in the organization the importance of following published policies and procedures and some basic patient health information security best practices. By having a work force that supports the organization's security goals, all the other administrative, technical and physical controls will become more effective.

Contingency Plans: Only as Effective as Their Last Successful Test

Incident management, business continuity, and contingency plans should have been developed during the initial compliance effort. These plans are only effective when they are tested and updated to reflect changes in technology and operations. According to the HIPAA security rule, these plans should have had predefined testing requirements. It is very important that these tests occur as scheduled and that any problems are corrected and written into updated plans. If tests show a plan to be ineffective, then a compliance issue has been discovered. However, new plans can be difficult to create for organizations that are not focused on managing emergency technology operations.

Patient Care Always Comes First

A healthcare organization's primary focus is obviously on patient health, not on information protection. The best solution to most organizations' compliance problems is to create a partnership with a trusted professional resource. In many cases this can be the same organization identified to provide ongoing security health checks.

Staying current with information security requirements is a difficult task for regular IT staff already busy with daily operations. The HIPAA security committee should help develop a relationship with its trusted adviser to identify technical, planning, and educational strategies to ensure continual diligence in protecting patient information. A good partner should be able to:

- Provide protection technologies at every level of the infrastructure that are reliable, scalable, and manageable
- Develop and host security awareness training tailored to the healthcare setting

- Understand how to quickly develop meaningful contingency plans and provide valuable knowledge transfer to response teams
- Assist with the policy and procedure development necessary to support new administrative, technical, and physical safeguards

Since HIPAA security requires continual diligence, resources must be devoted to ongoing compliance. Sharing HIPAA compliance responsibilities allows for a majority of an organization's resources to remain focused on patient care. And that's right where they belong.

Stephen C. Brown *(sbrown@iss.net) is a security consultant for Atlanta-based Internet Security Systems.*

Article citation:
Brown, Stephen C. "HIPAA Security: Don't Disband the Committee Just Yet." *Journal of AHIMA* 76, no.5 (May 2005): 52-53,57.