June 20, 2005

The Security Rule: There's Still Work to Be Done

By Kim M. Norton

For The Record
Vol. 17 No. 13 P. 14

Using common sense and staying vigilant are the most effective means for compliance.

As shredders have become the appliance du jour and identity theft is steadily rising, the HIPAA security rule is more significant than ever. With the passing of the April 21 deadline for complying with the rule, some organizations are struggling with maintaining compliance.

When implementing the specifications of the security rule into your organization, common sense is king. It is critical to regard the security rule as more of a guideline than an absolute, keeping in mind the organization's individual goals within the restrictions of the rule. In addition, being available to your staff and acting as an integral member of the team is as effective as any safety procedures you can institute, according to Carol A. Quinsey, RHIA, CHPS, AHIMA professional practice manager.

Shouldering the burden of maintaining compliance with the HIPAA security rule can be a daunting undertaking. If managing the task of complying with the rule is too much responsibility for a particular provider, there are outside security organizations that can assist. Additionally, there are numerous resources available to organizations that struggle with the rule, Quinsey says. "Use the AHIMA, use security companies, and most importantly read the security rule," she advises.

Terry Callahan, managing director of HIPAAT Inc. in Ann Arbor, Mich., helps organizations secure their nodes with software that authenticates the user and gathers audit information for each authorized session. Callahan stresses that the key aspect behind his security solutions is the audit feature. "Auditing is paramount. The security officer will have a time-synchronized overview of every node, even legacy modalities, within an organization to better maintain the security of protected health information [PHI]," he says.

"The 100% secure theory is a myth," Quinsey adds. "No one can be 100% secure." The goal of the security rule is to reduce the risk of intrusion and violation to an acceptable level the covered entity can live and feel secure with, she adds.

Becoming Compliant

In an effort to become compliant with the security rule, organizations that transmit data electronically (also known as covered entities) are required to analyze their risk and know where their weaknesses are, according to Quinsey.

"Notice the points of vulnerability, such as firewalls or inadequate passwords. Take measures to secure the vulnerability and document all the work that is done," Quinsey advises.

"Many organizations thought the security rule would go away, but they were wrong," she continues. "The security rule will not disappear and it shouldn't just be about HIPAA standards. It is simply good business to have a solid security plan in place."

The security rule involves following four safeguards: technical, administrative, physical, and organizational. Administrative safeguards consist of risk analysis, assigning a security management team, implementing security awareness training, establishing incident procedures, and addressing the language of both business associate agreements (BAAs) and any other contracts into which the organization has

entered.

Physical safeguards include establishing access controls, instituting a password system for workstations, and implementing device and media controls for all other machines in the organization. Technical safeguards focus on the installation of hardware and software on applicable nodes to control accessing and auditing programs. Organizational requirements necessitate the need for documentation of compliance in the organization's BAAs. It also requires that group health plans document that appropriate safeguards have been implemented in all areas where risk was accessed. Some standards exist under the safeguards, but the individual vendor can decide the way in which they are implemented, Quinsey says.

"There is not one correct way to approach compliance; it is all prescribed by each individual situation," Quinsey says. Although there are implementation specifications, she advises providers to develop compliance methods that suit their particular needs. "These specifications may or may not make sense for an organization's particular situation. Use common sense when applying the rule, but do not ignore the specifications. Every specification must be considered," she notes.

If the organization believes a certain specification under the rule does not make sense in its circumstances, it must document why it chose not to incorporate certain guidelines into its practice, she adds.

Staying Compliant

Once an organization becomes compliant, it is essential for it to remain compliant. When securing the four safeguards in an office, it is important to revisit the policies and procedures to ensure that the mandate matches the technology, Quinsey explains.

She points out that the security rule is driven by patient complaints.

"The HIPAA police are not monitoring or demanding updates. The likelihood that an issue will present itself is unlikely, but it could happen," she says.

With this realization, it is vital to keep abreast of the technology and security solutions you have chosen for compliance. In some situations, this may involve contracting an outside security solutions company to assist in maintaining compliance.

HIPAAT helps organizations become and stay compliant with security once a detailed risk analysis has been completed and a security officer has been appointed. Callahan assists in securing nodes by implementing the following three key features, according to Integrating the Healthcare Enterprise guidelines: instituting an access control/user authentication device, establishing node-to-node authentication, and installing software to audit all actions on each node.

"In this way, all nodes are secure and create a secure domain to satisfy the security rule," Callahan explains. "Then, for proper audit controls, the following three key elements must be identified: (1) Who is the user? (2) Who is the patient? (3) What protected health information was created or accessed?"

As Quinsey points out, organizations must apply the security rule in a way they believe is best for their particular situation. Likewise, Callahan says, "some facilities may believe that if a node is in a private space with limited access, then there are safeguards already instituted; however, this notion of privacy may not extend to an ultrasound machine in a public area."

"Because hackers are getting smarter, the technology must also get smarter and become more secure," Quinsey says. However, common sense is important here as well, and in some organizations, it may not be sensible to upgrade the current technology.

New machines will be equipped with software that already complies with the security rule, Callahan adds.

However, older nodes probably cannot be upgraded by the vendor because some of the older machines have moved out of production and do not warrant the development, testing, and installation of software, he adds. Most likely, the organization would address compliance with these older machines by using an alternative security method, such as installing a third-party solution, Callahan says.

Auditing and Incidents

"Auditing is key to enforcing the security rule," Callahan says. Auditing allows sanctioning of those who violate the facility's policies and procedures and is essential to maintain compliance.

One security solution Callahan supplies to vendors is an auditing tool kit to record and send security events from any node to a central repository database where the security officer monitors the information for security incidents. "Having a repository eliminates the need for the officer to go to each individual node to compile a security incident report," Callahan explains. To review the audit information, the security officer can search using the patient name, user name, or event.

"How we audit is important, but it is not as critical as who is monitoring it," Quinsey says. It is acceptable for the information technology (IT) department or an outside company to create the auditing program but department managers and supervisors must be involved in the process, she says. Additionally, the security officer, department managers, and supervisors should be involved in monitoring the data for incidents.

If a security incident does arise, the staff should know to whom it should be reported, Quinsey says. "Your project team for investigating security breaches should include IT, a department manager, and human resources to manage union-related issues," she says. "An administrator should not be included in the initial investigations because this is the person the report should go to."

Sanctions should be made depending on the severity of the infraction. In some situations, a verbal or written warning is sufficient. However, in others, immediate dismissal and notifying the police are required—especially in the case of identity theft, Quinsey says. "Take the appropriate action according to the procedures and policies that are in place," she adds.

"It is important to recognize when to first secure and then investigate the situation vs. investigating an incident then securing because some actions require different measures," Quinsey says. For example, if a patient's information is not secure, it is important to investigate the breach in security and then secure and act accordingly within the policies and procedures mandated, she says. No one's welfare is being threatened by a breach in secure information; however, this would obviously be different if someone walks into a restricted area wearing a badge that is not his or hers. In this case, it is important to secure the area first and then investigate. "Using common sense is essential when dealing with security incidents," she emphasizes.

Common Sense Compliancy

"Although there are standards, policies, and procedures within the security rule, never underestimate the power of talking to your staff," Quinsey says. "You would be surprised to hear the information that is divulged at a nurse's station." If you know what questions to ask and you have made yourself available to your staff, they will trust you, be open with you, and tell you more than a security program ever will about PHI security, she adds.

Also, managing your staff by walking around and being visible is essential. "Become familiar and comfortable with your staff. The more they see you, the more apt they are to trust and be forthcoming with you," Quinsey says.

Other Concerns

Another important safety precaution is to question what is in your organization's garbage. Sometimes doctors or nurses will print out a PHI for the patient to review, which is a normal procedure. However,

there is a security risk if this information is thrown out without first being shredded. “Everything dealing with a patient must be shredded before it is discarded,” Quinsey says.

To further keep track of the paper trail, she says it is important to ask how often the printer is emptied of unwanted reports that pile up. These reports are in an open forum for anyone to see; therefore, you must take the appropriate steps and be sure that all printed material is properly destroyed, she adds.

“Revisit the language of your BAA annually and address upgrades or changes to your equipment,” Quinsey says. Determine whether the language is accurate and reflective of the technology. “A BAA can become stale if it is not reviewed annually,” she adds.

Ongoing Initiatives

Even if a security issue is intangible, it should be addressed. Also, it is critical to recognize that implementation of safety measures is a continuous effort. “New procedures are implemented, new employees are hired, and new machines are acquired. All of these factors must be incorporated into the existing set of policies and procedures,” Quinsey explains.

In the aftermath of the security rule, it is important to have ongoing training to keep your staff vigilant of security matters, Quinsey says. “Not only will continuous training raise security awareness, but it will also alert your staff to changes and issues that may arise,” she says.

Ongoing training can be impromptu. For example, a scroll on a computer screen can be used to remind employees to not leave terminals unlocked and available for anyone to access. Also, a weekly notice of a security rule fact can be posted to keep your staff alert. Security issues should be addressed on a daily or weekly basis rather than a quarterly or annual basis, Quinsey says.

“In light of the security rule, it is important to realize that no matter how strong our passwords are or how secure our firewalls are, people are the weakest links,” Quinsey says. “Although the security rule is grounded in policy and procedures, it is essential to look at the people within your organization and know who is working for you.”

To further tighten security, Quinsey advocates mandatory background checks on every employee. “Managers need to know with whom they are dealing,” she says. “It is important that we are aware of a person’s background to know what type of people are reviewing confidential information.”

— Kim M. Norton is a freelance writer/journalist.