Proof Is in the Policy

Save to myBoK

by Tom Walsh, CISSP

Proving security compliance later requires establishing documentation now. HIM professionals have a valuable role to play.

HIM professionals played central roles in their organization's privacy efforts, ensuring that appropriate policies, procedures, and documents were in place. Now, just as much of the burden for HIPAA privacy was left to HIM, much of security compliance will be the responsibility of information technology (IT) departments.

Security compliance will be met largely through the implementation of policies, procedures, plans, and other forms of documentation. Given their strong background in documentation, their firsthand knowledge of process and procedure, and their experience in privacy compliance, HIM professionals have a lot to share with their IT colleagues. And those who get involved in security compliance can be unique and valuable assets to their organizations and to patient privacy.

This Much Is Clear: Document

The security rule is not as prescriptive as the privacy rule. The security rule tells covered entities what to do, but it does not tell them how to do it. Each covered entity must determine how to implement security based on its own risk analysis. However, one thing is very clear: documentation comprises a significant amount of proof of compliance. In fact, approximately 80 percent of meeting HIPAA security rule requirements involves implementing policies, procedures, plans, or other forms of documentation (see "Get the Message?" below.

IT departments setting out to meet compliance standards may not have a deep well of experience to draw from. Until HIPAA, what regulatory requirements have IT departments had to meet? Those of the Joint Commission on Accreditation of Healthcare Organizations (JCAHO)? Not really, because JCAHO's Information Management standards focus more on HIM departments than IT departments.

IT departments will face a second challenge: many IT people are not proficient in documentation. This is a bold claim, and certainly there are exceptions to any generalization. But the simplified truths are that IT professionals have an aversion to paperwork and documentation in general, and HIM professionals have a knack for it. And by their very jobs, HIM professionals already know what many IT professionals may have yet to truly experience—documentation and healthcare are inseparable. Thus, in the world of security compliance, the HIM professional's documentation expertise can prove a very valuable resource.

Get the Message?

There are three categories of safeguards comprising the HIPAA security rule: administrative (ß164.308), physical (ß164.310), and technical (ß164.312). Of the standards and implementation specifications listed in those sections of the rule, approximately 80 percent can be met by implementing some type of policy or procedure. In fact, the phrase "implement policies and procedures" appears 20 times in the rule, as follows:

ß164.308, Administrative Safeguards: 12 times
ß164.310, Physical Safeguards: six times
ß164.312, Technical Safeguards: two times

Note: This does not imply that a covered entity must create 20 policies or procedures. Some organizations choose to create fewer policies by combining several topics into a single, long policy. Other organizations prefer a greater number of shorter policies.

In addition to the number of times "policies and procedures" is listed under the three safeguard sections, ß164.316 of the rule, "Policies and Procedures and Documentation Requirements," requires covered entities to "implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart. . . ."

Can You Recommend a Good Policy for That?

For each security standard or implementation specification, HIM professionals can help the IT department determine the form of documentation appropriate to establishing compliance. "Documentation for Security" provides examples of the documentation that may be used to provide evidence of compliance with the HIPAA security rule standards and implementation specifications. Many of these documents may be adapted from existing privacy documents.

Prior experience is invaluable here, and HIM professionals should be certain to leverage their privacy work. For example, organizations may have already implemented some of the following policies, programs, and procedures:

- Sanction policies
- Training and awareness programs
- Procedures for reporting privacy rule violations (this same process could be used for reporting security incidents—after all, a breach of privacy may have been a result of a failure in a security safeguard or control)
- Business associate contracts or agreements (where protected health information [PHI] was being shared outside of the organization has probably already been identified)
- Workstation policies (policies that address the location of workstations and the implementation of privacy screens to prevent incidental disclosure of PHI may already exist)
- Media policies (policies on the storage and secure destruction of documents containing PHI may already have been instituted)
- Inventory of systems that process or store PHI

As noted above, the security rule fails to provide any way to measure or validate the quality of compliance, thus making "compliance" a subjective term. There is a difference between having a policy and having a good policy, of course, and knowing how to write a good policy is a vital step. Be certain to review the benchmarks of a good policy and study proposed security policies accordingly.

Lack of documentation does not mean that good security practices are not being followed by the IT department. In some instances it may simply mean that you and your IT department speak different languages. When working with IT staff, be sure to clarify what you mean. For example, you may ask the IT department, "Do we have policies for workstations?" The IT staff may acknowledge that they use policies for workstations, but they may look at you funny when you ask to see the document. To an HIM professional, a policy is a document. To an IT professional, policies often refer to the security settings that are displayed on computer screens during initial system installation.

A View from the Trenches

Beyond documentation skills, some of the most helpful insights that HIM professionals can offer spring from a basic reality: proximity. The high demand for space within healthcare settings often forces IT departments to be located away from the primary facility and physically isolates them from the rest of the organization. The result may be that IT staff operate with a disadvantage when it comes to fully understanding operational challenges.

HIM departments, on the other hand, are usually located within the primary facility. (Although with the growth of the electronic health record, the HIM department's location becomes less critical.) HIM professionals interact on a regular basis with physicians and clinicians, and they probably have a closer rapport with these staffs than do IT staff. This familiarity results in better understanding of the operational practices within the organization. HIM professionals are well aware of each point at which PHI is processed, shared, and stored—those points that demand risk analysis by the IT staff because they represent potential for accidental or intentional compromise of confidentiality.

In addition to helping IT professionals understand processes, HIM professionals can help ensure that security safeguards and controls adequately protect patient information without hindering healthcare operations.

The HIM department can lend experience and expertise to the establishment of security policies and procedures on the following topics:

- **Information access management.** Provide recommendations on who should have access to PHI and the level of privileges a work force member needs in order to perform his or her job. Many organizations are implementing role-based access controls, and the HIM professional's knowledge of the organization can help with this project.
- **Access control—printing of PHI.** Determine where printing restrictions should be implemented and recommend who should have print capability.
- **Audit.** Review audit logs and determine if any access to PHI was inappropriate or unauthorized. Or recommend which manager within the organization should perform reviews.
- **Integrity.** Identify location of correct information of interfaces linking data from various information systems get out of synchronization. HIM professionals may also be aware of shadow records and how they affect integrity.

The HIPAA security rule applies to work performed in locations outside the organization. HIM departments were among the first departments to have staff working off site. It has also been common to have services such as transcription and coding performed remotely. Thus, HIM departments are likely to have already implemented policies and procedures addressing the issues of a remote work force. Organizations may wish to use or modify these policies and procedures to address other off-site workers with remote access.

More Ways to Get Involved

In addition to sharing their experience, skills, and knowledge, HIM professionals can also get involved in establishing security compliance in the following ways:

1. **Read the HIPAA security rule.** Like the privacy rule, the final security rule includes a preamble, providing the government's answers to comments and rationale for the changes from the proposed security rule, released in August 1998. If you don't have time to read the preamble, start at the rule itself, sections 164.304 through 164.316.
2. **Maintain a good working relationship with the information security officer and IT staff.** If the two staffs don't already have a relationship, the HIM department might initiate one by inviting the IT staff to a breakfast or lunch meeting.
3. **Learn more about information security.** Perhaps the IT staff could loan one of their favorite books or could recommend Web sites on information security. The National Institute of Standards and Technology (NIST) offers free documents on information security in its Special Publications 800 series. Several of these documents—such as SP 800-30, "Risk Management Guide for Information Technology Systems"—are referenced in the security rule. For more information on NIST SP 800 series, go to http://csrc.nist.gov/publications/ nistpubs.
4. **Become a champion for security.** Leverage the department's relationships with clinicians and physicians to promote information security. Participate on the organization's security task force or advisory committee and offer experience.
5. **Participate with risk assessment and analysis activities.** Validate that policies and procedures address the primary risks to PHI and that policies are being followed.

When it comes to proving compliance, documentation is at the heart of the new security rule and thorough knowledge of processes will be invaluable. Those are topics that HIM professionals know a thing or two about.

Documentation for Security

HIPAA Security Rule Standards and Implementation Specifications	Policy	Procedure	Plan	Other	Examples of Other Documentation
Administrative Safeguards					
Security Management Process					
Risk Analysis				X	Risk analysis report
Risk Management		X			
Sanction Policy Information System Activity Review	X X				
Assigned Security Responsibility				X	Job description; memo
Work Force Security					
Authorization and/or Supervision		X			
Workforce Clearance Procedure		X			
Termination Procedures		X			
Information Access Management					
Isolating Healthcare Clearinghouse Function Access Authorization	X				
Access Establishment and Modification					
Security Awareness and Training	X			X	Syllabus
Security Reminders				X	Awareness handouts
Protection from Malicious Software				X	Awareness handouts
Log-in Monitoring				X	Awareness handouts
Password Management	X			X	Awareness handouts
Security Incident Procedures		X			
Response and Reporting	X			X	Incident report form
Contingency Plan			X		
Data Backup Plan			X		
Disaster Recovery Operation Plan			X		
Emergency Mode Operation Plan			X		
Testing and Revision Procedure Applications & Data Criticality Analysis		X X		X X	Results from testing List of critical applications
Evaluation		X		X	System certification
BA Contracts/Arrangements					

Written Contract or Other Arrangement				X	Contracts
Physical Safeguards					
Facility Access Controls					
Contingency Operations			X		
Facility Security Plan			X		
Access Control and Validation Procedures		X		X	Visitor sign-in sheets
Maintenance Records				X	Records such as work orders
Workstation Use	X				Workstation use and security could be combined into one policy.
Workstation Security	X				
&nsbp; Device and Media Controls	X				
Disposal		X		X	Form or checklist
Media Re-use		X		X	Form or checklist
Accountability		X		X	Form or checklist
Data Backup and Storage		X		X	Form or checklist
Technical Safeguards					
Access Control					
Unique User Identification	X				
Emergency Access Procedure		X			
Automatic Logoff	X				
Encryption and Decryption				X	Guidelines
Audit Controls				X	Audit reports
Integrity					
Mechanisms to Authenticate ePHI					Results from testing
Person or Entity Authentication				X	Results from testing
Transmission Security					
Integrity Controls				X	Results from testing
Encryption				X	Results from testing

***Tom Walsh** (twalshconsulting@aol.com) is the president of Tom Walsh Consulting, LLC, in Overland Park, KS.*

Article citation:
Walsh, Tom. "The Proof Is in the Policy." *Journal of AHIMA* 75, no.2 (February 2004): 24-28.