26.2-mile Security Rule: Is Your Organization Gaining on Compliance or Just Running in Place?

Save to myBoK

by Tom Walsh, CHS, CISSP

The race to security compliance is a marathon, not a dash. Here's how to gauge your progress.

With implementation of the HIPAA security rule next month, many organizations are preparing to sprint toward the deadline. However, compliance is more like a marathon than a 100-meter dash. Winning organizations are the ones that maintain their steady pace toward security compliance. Think of it as Kaizen, the Japanese strategy of continuous improvement. A key principle of Kaizen is improvement by gradual, incremental change rather than by sudden and radical measures.

Gauge your progress by reviewing the following checklist. Make sure you're not wasting energy or taking detours that are adding miles to the course.

Security Responsibility		
You're on course if you have… • Created a job description for information security responsibilities • Assigned responsibility for information security and announced the person's name and contact information to the work force • Created a task force or committee for information security	**You're falling behind if the person assigned responsibility for security...** • Has other job responsibilities that take precedence over information security • Would rather focus on technical controls before creating policies or procedures that will drive technology solutions • Cannot be identified by the general work force	
Risk Analysis		
You're on course if you have... • Identified the 10–15 major applications supporting the organization's business operations that have the highest potential for organizational risk (such as clinical, financial, and transcription systems) • Identified the five to six general support systems that share common functionality with other applications and are usually under the control of the IT or IS department (e.g., network, computer workstations, and mobile computing devices) • Created risk reports that document the most probable threats, existing controls, and vulnerabilities for each of the major applications and general support systems and rank the risks based upon probability and impact • Documented management's choices regarding how the risks will be handled	**You're taking a detour if you are...** • Debating what type of risk analysis tool to purchase • Trying to assess the risks to every application and system that processes and stores PHI rather than focusing on the most critical applications and systems first • Trying to remediate all risks rather than documenting management's decisions for handling risks	**Tip:** Management has three choices with regard to handling risk: 1. Implement a security control to reduce risks to an acceptable level 2. Transfer the risks (e.g., outsource the operations) or purchase insurance to offset the potential impact of the risks 3. Accept the associated risks for operating an information system in its current configuration Once an option is chosen, it must be documented.

Policies, Procedures, and Plans		
You're on track if you have… • Reviewed your current policies and procedures and identified gaps where modifications or additional policies are needed • Created new procedures, plans, or forms to supplement policies • Finalized and published the policies making them accessible to the work force	**You're running in place if you are...** • Trying to create a separate policy for each HIPAA security standard and implementation specification • Purchasing ready-made policies, slapping your organization's logo on the top of the page, and calling it done • Letting policy approval get bogged down as everyone debates exact wording rather than focusing on the policy's intent	**Tip:** Contrary to popular belief, you don't need a separate policy for each security rule standard or implementation specification. Keep it simple. Focus primarily on the information security policies that apply to the entire work force. Much of the compliance documentation could be incorporated into an IT or IS departmental policy manual or handbook.
Security Planning		
You're on course if you have… • Created a risk remediation or compliance plan • Created a budget for information security	**You're way behind if you...** • Haven't completed the tasks outlined	
Security Awareness and Training		
You're on track if you have... • Established a formal information security training program and documented staff attendance • Added information security content into new hire orientation • Sent out periodic security reminders and updates • Educated users on techniques for preventing malicious code such as viruses, worms, and spyware • Trained users on their responsibilities for logging off applications and for protecting unattended computer workstations • Taught users how to select strong passwords, with an emphasis on the importance of keeping passwords private	**You've left the track if you are...** • Looking for a one-size-fits-all solution for security training • Conducting training on information security for the sole purpose of meeting a HIPAA requirement • Still debating the content and delivery method	**Tip:** Maintain a file of security reminders distributed to the work force. This can be as simple as printing out e-mail messages and filing them in the notebook containing your HIPAA security compliance documentation.
Audits		
You're on course if you have... • Determined the audit capabilities of an application or an information system • Worked with application and data owners to determine which user activities and events should generate an audit log entry • Established procedures for periodically reviewing audit logs • Randomly reviewed records of information system activity, sometimes	**You're off course if you are...** • Planning on auditing everything • Not conducting random audits • Planning on keeping all of your audit logs for six years	**Tip:** Audit reports demonstrating that audits logs are indeed being periodically reviewed are the proof of compliance. Keep the reports for six years, not the actual audit logs. The audit logs should be retained based upon what makes good business sense. If the audit logs are ever part of litigation, then you may plan on retaining those

<table>
<tr><td>by employee and sometimes by patient</td><td></td><td>logs based upon your legal counsel’s advice.</td></tr>
<tr><td colspan="3"><b>Information Security Incident Reporting and Response</b></td></tr>
<tr><td><b>You’re on course if you have…</b>
• Established and implemented departmental contingency plans or procedures for conducting business in response to temporary outages of information systems
• Created a data backup plan and have at least one set of backups stored off-site for your critical applications and systems
• Documented your plan for restoring your information systems and keeping the business going in the event of a disaster</td><td colspan="2"><b>You’re falling behind if...</b>
• A formal business impact analysis has not been conducted to define and prioritize the major business functions and the infrastructure that supports them
• There is no written disaster recovery plan
• Your organization’s attitude is, “Well, we’ve never needed a disaster recovery plan before...”</td></tr>
</table>

While the security rule provides some standards for compliance, it does not provide universal solutions. Each organization must determine how best to meet the intent of the rule and then document its decisions and progress. To avoid getting bogged down in details or overanalysis of the rule, be committed to Kaizen. Steadily make progress and stay on course!

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

Article citation:
Walsh, Tom. "The 26.2-mile Security Rule: Is Your Organization Gaining on Compliance or Just Running in Place?." *Journal of AHIMA* 76, no.3 (March 2005): 24-27.