Health Information Compliance Alert

Training Strategies: From The Ground Up--Tips For Building Your Security Training Program

Use these simple guidelines to secure your organization's training.

Are you certain your employees have all the HIPAA security training they need to keep your organization sanction-free? If not, now is the time to fine-tune your security rule compliance, starting with an individualized training program built for your organization's specific needs.

Getting Started

While the privacy rule brought across-the-board mandates, the security rule "gives more room for individual development of a procedure that reflects the level of technology of the individual organization," says **William Hubbartt**, president of St. Charles, IL-based **Hubbartt & Associates**. Use this wiggle room to your advantage by developing a training program that works with the technology your organization uses, rather than trying to conform to one general standard, he suggests.

Prioritize: Your training program must incorporate the 18 required standards, but many of the addressable standards can also be used. "Build your program around the required standards," Hubbartt advises, and then choose the addressable standards that best suit your needs.

Generally speaking, the security rule "gives you an opportunity to speak to an audience [of employees]," reminds **Rose Dunn**, consultant at **First Class Solutions** in St. Louis, MO. "So if there are things that management believes are good to do regardless of whether the regulation requires them or not, this is an ideal time to incorporate them."

Set achievable goals: Security should facilitate your operations, not grind them to a halt. "If security paralyzes the goal of your business, then you've failed," clarifies **C. Jon Burke** of **Toshiba America MRI Inc.** "Don't let security paralyze the operations. HIPAA is not intended to interfere with the delivery of health care," he tells **Eli.**

Choose The Right Architect

Your security training program must be helmed by someone who knows how to bring your organization into compliance and has the technical knowledge to implement the necessary changes.

The designated officer also needs to possess "the ability to communicate with people who operate at all different levels of the organization," posits **Boston Bar Association** president and **Suffolk University Law School** associate professor, **Ren Landers**. Without effective communication, she says, the training will be inefficient and could lead to trouble.

Built-in flexibility: While the privacy rule requires you to have a privacy officer, the security rule does not specifically state that you must have a security officer," Hubbartt advises involving an information systems expert. "Depending on the degree of detail, there needs to be close coordination between" the security administrator and those qualified to carry out the compliance requirements, he says.

Most importantly, Landers observes, "it should be clear who ... people can go to at any time with questions so that there isn't this feeling that they're out there alone with decisions to be made that they don't feel comfortable making." In addition, Landers favors a policy that limits access to e-PHI until this doubt is resolved.

Identify The Crucial Elements

Security training "should be tailored to your organization and group of employees and the types of e-PHI they will have access to," explains Dunn. Each employee, from front line to management, comes into contact with different types of e-PHI and must be taught accordingly.

"Everybody should be trained," Hubbartt advocates, "and elements of that training may be more detailed according to the function of the employee." For those with limited access to e-PHI, he recommends that "the training be more broad-brush" by focusing on the requirements of the regulation along with the facility's objectives.

Trap: One of the most frequent pitfalls in security training, experts concur, is the belief that e-PHI exists solely on a computer. All those who have access to e-PHI must be trained and "that doesn't necessarily mean a person who has sign-on rights to a computer. It could mean someone who has access to disks or CDs because they transport that information from one office to another," Dunn clarifies.

And don't forget about training your maintenance or janitorial services staff, Landers cautions. All "people ... who might have access to equipment and who have control over access to locations where protected health information is stored" must be clear on what the limitations are. Failing to train them could result in serious security breaches.

Write it down: Also, make sure to maintain accurate documentation of your training. "The administrative director or other designated individual is responsible to maintain a record of training," reminds Hubbartt. Documentation can save you in the long run, says **John Parmigiani**, National Director of HIPAA Compliance Services for **CTG HealthCare Solutions** in Cincinnati, OH. "If there's an alleged violation somewhere down the pike, [documenting our training efforts proves] we attempted to get this across and embed it in our day-to-day operations."

Don't Overlook These Touches

"A solid training program is one that is not only ongoing, but also includes various awareness tools such as posters in break rooms, screen savers, mouse pads and other trinkets," says **Kevin Beaver**, consultant for **Principle Logic Inc.** in Kennesaw, GA. This will keep security from falling to the wayside.

Follow-up: Landers suggests frequent, small training sessions after the initial one "to refresh people's recollections about basic principles and practices that should be followed."

Keep it fresh: But it doesn't stop there--relevant training must occur in conjunction with changes in job function or modifications to the security regulation, or when a violation trend requires re-training. Dunn advises "a role-based reevaluation of what [staff members] have access to" when considering how to prepare employees for non-lateral moves within the organization.

Employees need "some overall sense of how they fit into the big picture [and] really good training on the questions or issues that are likely to come up and what the appropriate responses are," Landers says. Those issues will change as the technological environment changes, and the training schedule should accommodate that.

Assess The Package

The key to training retention is capturing your employees' interest while providing a little entertainment at the same time. Security is no different. "Government regs tend to be very dry and very dull and most people just tune out," Hubbartt notes.

Strategy: Therefore, you must make the training "interesting and applicable to their situation," he says. "Part of what I do as a trainer is try to cite case examples of instances that relate to the topic that I'm presenting because then all of a sudden people take notice," Hubbartt explains.

Another good idea: Dunn suggests using a quiz to determine how much of the training has been absorbed and what

needs to be clarified. These tests can be "done either at the time of the training or [after] the employee is allowed to return to their work-site" and should be situational versus fact-based. "Situational ones are more effective," she expounds, "because they encourage the employee to apply the concepts that they've been taught at the training session to a real life setting."

Bottom line: The security administrator(s) must allow for modifications and adjustments within their training programs, as well as several re-training sessions, that reflect alterations to the regulations. Because regs aren't etched in granite, they can and will be modified as the **Department of Health and Human Services** determines the flaws.

"Use common sense," when developing your training program, Burke advises. While the primary goal of security rule training is accordance with the law, "the most important one is making sure patients' rights are protected," Hubbartt says.