Codify
BY AAPC

Health Information Compliance Alert

SECURITY STRATEGIES: 9 STEPS FOR COMPLETING YOUR SECURITY RULE COMPLIANCE PROGRAM

Be sure you've sorted through each standard - before it's too late

The April 20 security rule compliance deadline is just a few weeks away. Would you bet on your compliance program?

Don't gamble with your security rule compliance - or your patients' PHI. Use this guide to ensure you haven't overlooked any crucial compliance components.

1. Create a security plan. "You need to know where your PHI sits at rest, where it enters your facility and how it leaves," asserts **David Szabo**, a partner with Nutter McClennen & Fish in Boston.

This inventory should include all devices, including portable or wireless ones. And it must account for both electronic and paper PHI.

2. Conduct a risk assessment. Once you take stock of all your devices and information, you must assess the risks. For example, if you plan to exchange PHI electronically but you don't have a firewall, then there's a huge risk that your information will be intercepted, Szabo says.

After you uncover your risks, prioritize them by most critical to least critical, suggests **Shenethia Jones**, security officer for Texas Health Resources in Arlington. Attack your most dangerous vulnerabilities first.

3. Determine who will be responsible for your security compliance. Your security manager doesn't have to be one person, says **Raj Patel**, the manager for security assurance and consulting at Plante & Moran in Southfield, MI. Rather, you could develop a security team.

Important: If you decide to go with a security team, make sure each member understands exactly what he or she is responsible for, Patel stresses. And remember, your security point-of-contact can simply manage other staff members' compliance activities.

4. Establish and monitor your termination procedures. Your termination procedures are crucial to eliminating the chance that a disgruntled ex-employee will get his hands on patients' information, experts concur. That means you must have a smooth process for blocking employee access - whether planned or due to an emergency, Patel notes.

5. Create a formal access authorization process. Whether you're bringing in new employees or shift staffers from one department to another, you need a streamlined process for both requesting and granting access rights, Patel says.

For example, your security officer or team may set up access levels or categories based on job function. The department heads could then request that a new member be granted access based on the duty she will perform in the department.

Remember: You must make this process part of your written policies and procedures. Failure to produce a written guide to your access process could land you in hot water if there's a breach.

6. Streamline your security incident response procedure. Security incidents range from a ping on your firewall to someone stealing one of your workstations. The security rule demands that you develop a process for spotting these incidents, responding to them and mitigating any harmful consequences, Szabo says.

Important: You must have a response procedure in operation by April 20, declares **Mark Eggleston**, HIPAA Compliance Program Manager for Health Partners of Philadelphia. "But your procedure doesn't have to be perfect - you can always revise it over time," he adds.

And, be sure your legal team reviews your incident response procedure, Patel recommends. That way, you can be sure your plan will protect your entity's legal best interests.

7. Create and test your disaster recovery and backup plans. You must map out how your organization will respond to a disaster, Patel says. For example, if your facility were slammed by multiple hurricanes in one season (think of Florida last fall), how would you protect your patients' information? (For more information on disaster recovery planning, check out **HICA** Vol 4, No. 11.)

Tip: Don't wait for a disaster to run through your plan. Conduct at least one test drill before April 20.

8. Conduct security awareness and job training. Your staff needs to be educated on the perils of poor security and how to avoid them. This general security training can then be used to carry out more specific, job-focused training that will explain to staffers how to perform their jobs securely, Eggleston says.

9. Turn on your audit controls. Your audit controls serve several purposes. They allow you to detect and deal with problems before a breach occurs, they provide forensic evidence after a breach and they act as a deterrent for your workforce members who might have the urge to spy on friends' or family members' records.

Even weak auditing systems can be highly useful, Eggleston says. For example, your system might only give you a list of which users are in your system at a given time. You can always compare that to a list of who managers say should have access - making the audit more thorough.

THE BOTTOM LINE: Your security rule compliance program should be in the final stages of completion. But, if you haven't worked through each detail of the regulation's standards, you'll still be in a good position to fend off a violation if you can show that you have worked hard at least to implement these 9 components.