Health Information Compliance Alert

Security: 4 STRATEGIES TO EASE YOUR SECURITY RULE ANXIETIES

Eli's experts help you get over the top security rule humps

One thing about the security rule is clear - it's up for interpretation. Before you spend another minute banging your head against your desk, try these effective strategies for clearing the top four security-rule hurdles.

1. CUSTOMIZE THE RULE

"The industry is confused about how much has to be done for security-rule compliance," explains **Jeff Boyer**, HIPAA Compliance Coordinator for the HIPAA DC Program Management Office in Washington, DC.

The problem: There is no playbook for compliance. That may lead you to take the most extreme measures to be as safe as you can possibly be, Boyer says. "The trick is it takes a lot of money to get there," he adds.

The solution: Find a compromise between what you could do with an unlimited budget and what you can accomplish with your actual budget, Boyer advises. Example: To protect your patients' electronic PHI, you could encrypt your entire system. However, that could cost hundreds of thousands of dollars. A more feasible method of protecting patient information might be to use encryption at your entrance points - like your firewall or e-mail - and then enforce a strong password policy, such as using a number-letter combination and swapping passwords every 30 days, he suggests.

2. COMPROMISE WITH YOUR TRADING PARTNERS

While it isn't necessary to sign a business associate agreement to share information with your patients' other treatment providers, you can't just send PHI out into the world without ensuring its security. This is where the trading partner agreement comes in (see Trading Partner Agreement).

Once a covered entity signs your trading partner agreement, that organization is bound to your expectations for privacy and security, explains **David Szabo**, an attorney with Nutter McClellen & Fish in Boston.

The problem: "Your trading partners may resist applying your standards," Szabo says. Why? If you're swapping information with a larger organization, you probably don't want to be contractually bound to their security standards. And if the organization is smaller than yours, you'll have a hard time getting them to comply with your security rules, he explains.

The solution: Work with your trading partners' tech team to find some middle ground that won't break either organization, he says. Example: It's not feasible for you to give each employee a biometric token, but you can enforce a stronger password policy, he offers.

3. OPEN YOUR ROLE-BASED ACCESS UMBRELLA

You don't have to define a role for each employee to access your patients' PHI, says **Fred Langston,** a principal with VeriSign in Seattle. Rather, define who can access PHI by thinking in terms of groups of employees, he suggests.

Best approach: Create one role per department rather than a separate role for each employee within a department. Then make exceptions for the handful of employees who may need a different level of access, Langston offers. You'll end up with more concise access controls, he says. Bonus: This will make it easier to track access, Langston notes. "You can audit per role rather than per employee - that will save you loads of time," he says.

4. LINK UP YOUR SECURITY INCIDENTS

Are you gearing up to launch a full-force attack on all suspicious activity that crosses your path? That's more than you need to do, Langston tells **Eli**. To determine when a security incident is worthy of a full response, search for a larger pattern among all the layers of security you've built for your organization, he counsels.

Example: If you or your employees pick up a suspicious event, check your activity logs and firewall for similar activity. You should investigate all strange activity, Langston says. But you only need to get your incident response team involved if you find that correlation, he says.

THE BOTTOM LINE

The security rule was built to be flexible, experts agree. That means the steps you take to put your organization into compliance must reflect the size, scope and sophistication of your operation.

No one can be 100 percent secure, Szabo reminds. You have to decide how much risk you are willing to accept, he says. And once you've determined that level, you need to take reasonable - not extreme - steps to meet it.