Codify
BY AAPC

Health Information Compliance Alert

SECURITY COMPLIANCE: ERADICATE THESE RISK ASSESSMENT MYTHS

Here are the top 5 myths - and the real truth behind them

You've worked tirelessly to train your employees to secure your patients' confidential medical information - but some misconceptions are harder to shake than others. Here are the top five risk assessment falsehoods - plus some expert advice to set your staff straight.

MYTH #1: 'Only top management is responsible for assessing our facility's threats and vulnerabilities.'

FACT: Include your entire workforce in the risk assessment process, because they will provide you with valuable information, counsels **Miriam Paramore,** a principal with Paramore Consulting Inc (PCI) in Louisville, KY. Try this: Build a cross-departmental team comprised of key workers at different management levels, she suggests.

"It's a big challenge to organize the work and get the level of results you need" to secure your patients' PHI, Paramore explains. By getting your entire staff involved, you can better divvy up the workload for more complete results, she adds.

MYTH #2: 'We've completed our risk assessment, so we're security-rule compliant.'

FACT: Compliance with the security rule is not a one-time event. Rather, "it's a culture and a process" and is ongoing, acknowledges **Patricia Markus,** an attorney with Smith Moore in Raleigh, NC.

Remember: A risk assessment is never really complete, since new threats and vulnerabilities will pop up all the time, Markus says. That's where monitoring comes in - "a few months down the line you have to ask 'Are we still complying with this provision? Are there better steps we can take? What new threats do we have?'" she notes.

And you "don't want to get married to your first attempt at a risk assessment," stresses **Frank Ruelas,** compliance officer at Gila River Healthcare Corp in Sacaton, AZ. Look at what you missed or left out and then adjust your risk assessment as you go, he advises. That way, you tailor your assessment to your risks - not the other way around, he explains.

MYTH #3: 'We should conduct a risk assessment and implement changes without ant outside help.'

FACT: It is entirely possible to do your own risk assessment, but you shouldn't shy away from seeking help from other organizations or consultants, Paramore asserts.

Your tech team or other security-savvy employees may be true experts, but the insider's-eye could work against you. "It's highly likely you'll find blind spots in an internal member's review of your entity's compliance" that would be obvious from a fresh perspective, Markus explains.

And, bringing in someone from the outside to help with your security rule compliance will look good to CMS if there's a security breach down the line, Paramore notes.

If you buck at the idea of working with a consultant rather than doing an in-house risk assessment, work with an expert to complete the assessment. This type of team effort will "show you took your security rule obligations seriously," she says.

MYTH #4: 'We don't have to worry about the addressable implementation specifications

FACT: You can't just focus on learning the standards and ignore the addressables, Paramore advises.

Remember: While you don't have to learn and master each of the addressable standards, you do need to train for each security measure you've decided to implement - regardless of that control's place in the pecking order, Markus says.

MYTH #5: 'We did a gap anayalsis already so we don't need to do a risk assessment.'

FACT: "This is just not true," Markus stresses. And you have to be able to differentiate between the two if you want to do a thorough job of either, she warns.

Think of it this way: The gap analysis measured the difference between what you were doing versus what the privacy rule requires you to do. On the other hand, a risk assessment demands that you weigh your threats and the risks they pose to your organization, Markus says.

This distinction doesn't mean the gap analysis and risk assessment don't dovetail, Paramore notes. When you combine your gaps with your potential threats, you have a solid plan of action that will conquer your privacy and security rule compliance goals - and determine how each staff member's work duties and behaviors must change, she affirms.

LESSON LEARNED

Like all components of the security rule, you must conduct a risk assessment that is reasonable for your organization's size, scope and sophistication, Paramore assures. And don't be afraid of moving in the wrong direction, Ruelas counsels. "Once you start, you'll have a better idea of where to go," he assures.