Codify
BY AAPC

Health Information Compliance Alert

HIPAA Compliance: Do You Have An Information Security Management Process?

Tip: Run your data security like a business.

If you don't have a formalized process in place to manage your data security, your HIPAA Security Rule compliance is in serious jeopardy not to mention the chance that you'll face a not-so-favorable audit. Here's what you need to do to create an airtight information security management process.

According to HIPAA expert Jim Sheldon-Dean, founder and director of compliance services for Lewis Creek Systems, LLC in Charlotte, VT, an information security management process essentially protects:

- Confidentiality;
- Integrity; and
- Availability.

Important: You must "have some kind of a security management process ... not just regular reviews," Sheldon-Dean stresses. You need to "really understand what's going on."

Get into a Business Mindset

Scenario: Think about running your security management process like a business. In a business, you need to "have some kind of regular business process where you're making changes based on making as much money as you can," Sheldon-Dean says.

Just like a business would have a process in place for continuing profits, you need to have a security management process in place for continuing security. "That's where you do your information flow analysis and understand who has access to things, what's been going on in your networks and systems," Sheldon-Dean explains. "And do regular audits and reviews just as you would in your regular business."

If your business makes widgets, and you have a competitor that is opening up a new widget factory down the street, you would likely have a meeting to figure out how to deal with the situation. Or you would try to find out whether your business has problems.

"Then under the security scenario, you're making changes based on improving your risk profile, reducing risks, and improving your confidentiality, integrity and availability," Sheldon-Dean states.

Good advice: "And when something goes wrong, learn from it," Sheldon-Dean adds. "Any kind of incident, you can learn from it." Dissect what happened and how you can prevent the incident from happening in the future.

Perfect Your Security 'Balancing Act'

"Don't forget that when we talk about security, it's not just confidentiality," Sheldon-Dean reminds. "It's also the availability portion."

Understand: "Security is hard because it's a balancing act," Sheldon-Dean points out. "I mean, how do you have something completely confidential and completely available at the same time? You can't do it."

Consider this: Approximately 73 percent of organizations don't have enough trained personnel and other resources to prevent and detect information security breaches, according to the Third Annual Benchmark Study on Patient Privacy &

Data Security by The Ponemon Institute, released in December 2012.

The Ponemon study also revealed that information privacy and security are not "fiscal priorities" in the healthcare realm, which threatens an organization's reputation and operating costs, not to mention its patient data.

"Security is an impossible job," Sheldon-Dean continues. "That's why you need to think about all these things and come up with the best plan you can for your organization. That's why risk analysis is so important so you can find those balancing points."

Indeed, risk assessments play a crucial role in identifying potential threats to your organization, stated Raees Khan in "Practical Approaches to Organizational Information Security Management," a white paper for the SANS Institute. And they "provide a perfect opportunity to implement effective controls to protect critical processes and assets."

Why Your Security Policies are So Important

You'll need to put into place some security policies. "You wind up with a security policy framework where you have the policies that talk about your security management process and how are you going to control access and how you're going to manage your data as well as a user policy," Sheldon-Dean says.

Your security policy should provide one place for users to understand how they should manage the data, among other things. "The important thing about policies is they give you the right to do what you need to for compliance," Sheldon-Dean explains. "And this is [one] of the trickiest areas that you could ask about in an audit: 'What do you have in place for your policies and procedures?'"

Stay Flexible & Keep Pace with Changes

Ultimately, your security policy needs to give you the authority to be flexible and do what you must to meet changing needs, because your security needs will surely change as new devices, software and other evolutions come along.

Case in point: "I mean, who thought texting was going to wipe out paging a few years ago?" Sheldon-Dean asks. "And anybody who doesn't believe that texting is wiping out paging right now has got their head in the sand." So you'd better make sure that your policies will allow you to grow with such changes, or be prepared to change your policies.

"And have plenty of details in your procedures," Sheldon-Dean adds. "Keep your procedures as something you can modify on a regular basis."

Follow This Process Checklist

So as you're preparing your information security management process, keep this checklist in mind to ensure that you're covering all the bases and looking at your security issues from all angles:

- Define and understand what you have.
- See how well it performs.
- Watch for problems.
- Review activities and issues.
- Make changes based on "bang-for-buck."
- Perform information inventory and flow analysis.
- Create access and configuration controls.
- Know who and what's been going on in your networks and systems.
- Respond to and learn from incidents.
- Audit and review regularly, and when operations or environment change.
- Make risk-based improvements.
- Focus on: Confidentiality, integrity, and availability.