Codify
BY AAPC

Health Information Compliance Alert

Security Strategies: 7 Steps To Save Your Security Incident Ship

These suggestions will keep your security rule compliance efforts moving.

Knowing how to respond to a security breach is crucial to your office: It not only keeps your business running efficiently, but it reduces your chances of violating the security rule. Here's some straightforward help to keep you on the right track.

1: Spot your enemy. "Any time you know something has been compromised, you have a security incident," explains **Fred Langston**, security consultant with **VeriSign** in Seattle. And incidents include everything from computer worms and viruses to password theft to a stolen laptop, he points out.

But you don't have the time and money to investigate the range of suspicious activity the rule highlights. **Strategy:** Break the rule's security incident definition down to: a) the types of incidents you are at risk for; and b) how they would impact your facility, suggests **Chip Nimick**, Security Officer for the **University of Rochester Medical Center** in New York.

Tip: Group the security incidents your organization has experienced by type, Nimick recommends. Sort each type by how it affected your system. Next, describe what your level of response will be for each type of incident, he adds.

2: 'Fess up. After you know what happened, figure out "what went wrong, what could have been done to prevent it and what you will do to keep it from happening again," counsels **Robert Israel**, VP and CIO for the **John C. Lincoln Health Network** in Phoenix.

3: Make changes. "You have to immediately remediate any breaches that identify a weakness in your system," says attorney **Kirk Nahra**, a partner with **Wiley Rein & Fielding** in Washington, DC.

First step: Attack your policies first, Israel suggests. Ask yourself: "Do we have a policy that identified this? Was that policy followed? Was it inadequate? Do we need to write a policy to address this?"

4: Learn from your mistakes. "You aren't looking for a scapegoat, but you do need to avoid making the same mistake again," advises **Greg Young**, Information Security Officer for Mammoth Lakes, CA's **Mammoth Hospital**.

Tip: Schedule a training session immediately after a violation and use the violation as a practical example of what not to do, Young suggests.

5: Sanction and mitigate as necessary. "We discipline depending on intent and action," Israel explains. **Example:** A staff member who borrows someone else's password to complete a task might be given a verbal warning and retrained. A staff member who uses a password to steal patients' identities would be terminated and turned over to authorities.

Strategy: Train your staff to be aware of their coworkers' inappropriate actions and to report anything they think is fishy. Then you can catch problems before large-scale mitigation efforts are needed, Young notes.

6: Map out your general response. "We have a list of general incidents and how we'll respond to them," Israel shares. **Strategy:** Use the common security incidents listed below, and others you find in your office, to figure out how you will respond. Then schedule test drills until your office has the process down pat.

7: Document your steps. Keep a copy of your original policies and procedures on file, experts suggest. And don't discard your records that show steps you decided against, Young stresses. You must have proof that "you made an attempt to correct your entity's shortcoming rather than just shoving it under the carpet," he says.

Top 5 Security Incident Warning Signs

Your passwords stop working.

You receive messages that you are almost out of disk space.

Your computer crashes several times.

A computer that contains PHI is stolen from your department or home.

Someone tries to coerce you into providing your log-in information.