Health Information Compliance Alert

SECURITY COMPLIANCE: Don't Deep-Six Your Security Ship

Expert tips for smooth security incident sailing.

Need help understanding what a security incident is and what to do with it? Well, you're not the only one. Defined broadly in the reg as "attempted or successful" security breaches, just about anything could be called a security incident. Fortunately, **Eli's** HIPAA experts know what to look out for.

Keep Track Of Your Incidents

To catch the incidents that are potentially dangerous, **Ren Landers**, president of the **Boston Bar Association** and associate professor at **Suffolk University Law School**, promotes good documentation. "It's a good idea to keep track of what kind of things do happen" so that you can adjust your policies and systems to account for those vulnerabilities, she says. The security incident report can expose areas in which your security policy isn't thorough enough or where more manageable measures could be applied.

Look For Incident Patterns

Because there are malicious threats that must be realized and resolved, your incident reporting system should be equipped to catch them.

To ensure that all the little components of what could be a large problem are recognized, consultant **Margret Amatayakul**, in the Schaumberg, IL office of **Margret AConsulting**, advises "an organization over-report rather than under-report" their security incidents. **William Hubbartt**, president of **Hubbartt & Associates** in St. Charles, IL, agrees. "If you're going to err, err on the side of caution," he tells Eli.

Harry Smith of **Timberlyne Technologies** in Lakewood, CO suggests looking for trends in security incidents, such as repeated attempts to access your system's e-PHI in a short period of time. Taken separately, these attacks are innocuous, but when seen as part of a larger picture, as happens in a report, their true nature is revealed.

And with an incident tracking system in place, "if something actually happened, you've got enormous opportunities to try to mitigate anything bad resulting from that" before the compromised information is used maliciously, says **Kirk Nahra**, a partner in the D.C. office of **Wiley Rein & Fielding**.

Create Security Awareness

This is not the only advantage of security incident reporting. The incident report "creates a security awareness which actually reduces the number of incidents simply because ... it keeps security top of mind," Amatayakul asserts.

The reports will help administrators know where security training isn't being implemented or has failed. "If you don't keep track of how people are doing on implementing what you've trained them to do, then you don't know where your problems are and you can't prevent them," Landers warns.

Therefore, it's important to create an environment where employees feel comfortable documenting any incidents without worry. "Some people think that reporting an incident is like telling on somebody," Amatayakul says, but if it becomes "a way of life that we have to collect whatever issues we see so that we get them fixed," the reporting will be efficient and incidents could dwindle over time as security awareness improves.

Simplify The Process

To streamline and normalize the incident reporting process, Smith suggests the following steps:

- **Make the report.** Whether your organization chooses electronic or paper documentation, each incident must be recorded. Once that documentation has been made, it should be cycled through to those responsible for incident response.
- **Assess the damage.** "If you know damage is being done, your very first order of business is to stop the bleeding," Smith says. Damage control must be quick and applicable -- whether that means shutting down an entire system or re-training your staff.
- **Recover your operations**. Once you've isolated the violation, your organization can get back to work. Though it may be difficult to return to a state of normalcy after serious security breaches, policies should be in place to support that.
- **Investigate the issue.** With all operations running smoothly, the security official must determine what went wrong and who is responsible. "In theory, there should be no incidents. So, you need to find out where the vulnerability is that allowed [the incident] to happen," Smith says.
- **Resolve the incident.** You've assessed and controlled the incident's damage, and you've discovered how and where the breach occurred. Now you've got to make the necessary changes so that the incident does not happen again. This could mean changing your policies and procedures, or it could involve more sophisticated security networks.

As Hubbartt states, "in light of our market place and our world economy and our world political environment, any incident is a potential threat and we need to consider it seriously, evaluate it and act appropriately."