Health Information Compliance Alert

Security Compliance: Don't Let Security Incidents Catch You By Surprise

Expert guidance helps you spot incidents before the feds spot you.

You have to protect your patients' PHI from security incidents, but do you know how to recognize an "incident" when you see one? **Eli's** experts offer tips to help you and your staff detect incidents before they turn into major breaches.

Make The Rule Your Own

"Any time you know something has been compromised, you have an 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.

Wave The Red Flag

While you can't see every security incident coming, there are some obvious signals that will clue you in when your system has run into one. Example: If staffers' "passwords stop working, or their files disappear from the network," your organization could be in the middle of a breach, says **Jo Carey**, information security specialist at Albuquerque, NM's **Presbyterian Health Services**.

Tip: Train your staff members to call either you or another security point-person before they brush off these types of incidents, Langston suggests. Though it could turn out to be nothing, you need to be aware of possible security breaches so you can connect any dots, he says.

When your staffers report problems, your tech support group will be able to recognize patterns and quickly identify security problems.

The bottom line: Be open about security incidents with your staff, Nimick recommends. That way, you can provide practical examples of violations and help your staff learn to recognize signs of them, he says.

Also, be sure to educate your staff on what to do if they see something that could indicate a security breach--it could mean the difference between a small security incident and a major HIPAA violation, Carey says.