Health Information Compliance Alert

Security Compliance: Respond to Your Security Breach in 4 Easy Steps

Here's how your employees can help you thwart data thieves.

With the number of reported security breaches increasing every day, you can no longer assume your organization is immune to security attacks.

Use this expert advice to help your employees spot -- and stop -- potential security breaches before patients' data is exposed to criminals.

1: Recognize Your Trouble Zones

Spotting security breaches is a challenge, but you can teach your personnel to be on the lookout for obvious clues that something has gone wrong, says **Chad Markham**, information security officer for Mercy Medical Center in Sioux City, Iowa.

Training tip: Pinpoint the areas in your organization where users are most vulnerable to attack, and then train them to respond effectively. Example: Markham noticed that his users were most vulnerable through e-mail, so he launched an education campaign that helped staff sort safe e-mails from dangerous ones, he says.

Next step: Post a checklist of common security incidents in your staff areas. Be sure your employees know to sound the alarm immediately if those (or any other) suspicious activities are observed. Here's a short list to get you started:

•-Outright threat to PHI from an insider or outsider-(such as stolen computers);

•-Attempt at social engineering (such as someone-calling in for a password or asking a receptionist for-building access they don't need);

•-Virus outbreak;

•-Slow system performance, crashes, or lock-ups that-appear out of the blue;

•-Sudden appearance of unknown files on a system;

•-Strange file date/time modifications; and/or

•-Unauthorized account access, computer and/or network usage.

Remember to tailor your list to the types of security breaches most likely to occur in your organization, Markham says.

2: Refine Your Reporting Process

You will be better equipped to respond to a potential security breach if you plan and test a streamlined incident-reporting process, says **Chris Apgar**, president of Apgar & Associates, a security consulting firm in Portland, OR.

If you are in a large institution, you'll need to develop an incident-response team that can investigate the potential breach. Best bet: Task your information technology (IT) department with fielding and examining employee reports, Apgar suggests.

For small- to mid-sized organizations, you can train one or two employees to handle security reports. Important: Make sure your team members are comfortable with new technologies. You might also want them to earn certifications or otherwise become "specialists" in your heavily used applications. For instance, if Outlook is your e-mail client, and you are worried about viruses and malware attachments, your security point-person needs to become an Outlook expert.

After you develop your incident response team, you'll need to coach your staffers on the best method of reporting possible security breaches to the team. Good idea: Use the processes already in place. For example, Mercy Medical Center set up a help desk long before the security rule took effect. "If our staff members suspect availability or integrity issues, they e-mail or call the 'resolution center'," Markham says.

Here are a few options for your reporting process:

•-A help desk where calls and e-mails are answered as-they come in by a person dedicated to that position;

•-An e-mail account monitored by team members where-staff members can send their concerns;

•-A telephone line that is checked throughout the day-by your response team where staffers can leave-detailed messages; or

•-An incident reporting form that employees fill out-and then submit to the correct person.

3: Investigate the Incident

No matter which reporting process you choose, your response team must be educated on what to do with the incident reports they receive.

First step: Your team must determine whether a breach actually occurred. A thorough investigation -- which includes examining audit logs and system activity -- may reveal that what "appears to be a security incident is really just a malfunction of your software or hardware," Apgar says.

However, if the investigation reveals a successful or attempted security breach, your team must know who to alert. Try this: Create a contact list of key people in your compliance, business, and human resources departments. That way, when staffers uncover a breach, they can alert the right people--without wasting time hunting someone down.

Important: Teach your response team members to accurately document each step in their investigation, from their first warning to when they turn the incident over to the next level.

4: Consider Patients' Need-To-Know

The security rule does not mandate that you tell patients when their information is inappropriately accessed due to a security breach, but you do have to mitigate any possible damage patients may experience due to the breach, says **William Hubbartt,** president of Hubbartt & Associates, a medical privacy and security consulting firm in St. Charles, IL.

If the breach was significant -- perhaps Social Security or credit card numbers were accessed -- you should tell your patients so that they can monitor their credit reports or cancel their credit cards, Hubbartt says. Your patientsts' actions will also help you mitigate any further damage, he notes.

Best solution: Don't just warn your patients about the breach; tell them what you are doing to fix the problem. Give patients contact information for a staffer who can answer their questions and work with them to protect their PHI, Hubbartt recommends.

Remember that any inappropriate access of PHI must be recorded in each affected patient's accounting of disclosures, Apgar says. And your state may have its own rules about when you must inform patients about security breaches.

Tip: Don't wait for a breach to occur to educate your personnel to recognize and report security incidents. "You want to

hit the ground running -- not stumble around blindly -- when a breach is uncovered," Apgar asserts.