Health Information Compliance Alert

COMPLIANCE STRATEGIES: WATCH OUT FOR HIPAA ROADBLOCKS

Pave your way to HIPAA compliance with a security audit

You've developed policies and procedures to protect patients' PHI. That means you've reached HIPAA security rule compliance, right? Wrong. If you don't monitor your compliance efforts, you could be racing your way to disaster.

The privacy rule focused on physical protection of PHI, but the security rule mandates a much broader approach to protecting the privacy of your patient's health information, explains **Shenethia Jones**, security officer for Texas Health Resources in Arlington, TX.

START YOUR ENGINES

Not sure where to begin? Your security audit should naturally flow from your security risk analysis, asserts **Margret Amatayakul**, a consultant with Schaumburg, IL-based Margret A\Consulting. It will give "you a good idea of what gaps you have and the threats in your environment," she says.

Once you know where your threats are, you can establish a baseline to work from, Amatayakul insists. And, you can use your risk assessment to establish security standards that will apply across the board, Jones concurs.

NOT A ONE-WAY STREET

Though the security rule doesn't demand that you focus solely on physical security, it doesn't let you off the hook either.

Tip: Develop and distribute a facility security plan that your employees can easily refer to, suggests **William Hubbartt**, a consultant with Hubbartt & Associates in St. Charles, IL.

This plan will automate your facility's physical security process so that you can free up time for other compliance issues, Hubbartt says. It can also help you focus your efforts on which security measures are reasonable and which can't be done.

Remember: You must audit your facility's physical security, but you can't ignore technical security measures, Jones warns. "You have to ensure that the controls on an application or system are being applied correctly," she says.

DRIVERS WANTED

"Security officers must set and distribute the audit requirements" throughout your facility, Jones insists. Though the responsibility is delegated down the line, the security officer must ensure that HIPAA's security rule requirements are met, she says.

Good idea: Security officers should meet with team leaders to find out if any needs and threats are changing, Hubbartt suggests.

REMEMBER YOUR RIDERS

Work with your employees during the security audit process, experts agree. "You have to be up front about the audit," Amatayakul asserts. "Put people on notice that this will be occurring routinely," she recommends.

The goal is not to trap employees. **Tip:** Explain to your staff that "you're looking for problems that will harm data integrity or reduce their ability to [access] data," Amatayakul advises.

Putting a positive spin on audits allows employees to be honest about their problems, Amatayakul affirms.

There is, of course, a time and place for the surprise audit. "If you keep finding issues, and things aren't getting done the way they should, then surprise inspections are a good alternative," Hubbartt advises.

BEAT THE CLOCK

Though the HIPAA security rule doesn't set a timeline for monitoring, you can use your last audit or risk assessment to decide when to start the process. **Action plan:** Identify what you're looking for, note any discrepancies, and then set up a time frame for resolving them, Hubbartt suggests.

Tip: Daily or weekly monitoring is best for high-risk systems, Jones counsels. For everything else, customize your monitoring schedule to allow yourself and your facility enough time to work through issues, experts agree.

THE FINISH LINE

There are ways to manage monitoring security rule compliance without focusing all your time and energy on auditing.

Remember: "Our biggest problem is people, not technology. Technology is the solution," Amatayakul says. Keep your employees on board during the process and it'll be more rewarding for all involved.