Health Information Compliance Alert

Security Strategies: 5 Security Rule Misconceptions That Could Land You In Hot Water

Let our experts guide you through the security rule's gray areas.

Are you sure you're interpreting the HIPAA security rule correctly? Your HIPAA compliance program will need adjusting if you've fallen into any of these traps identified by our experts.

No Carbon Copies

Warning: Perhaps one of the costliest security rule misinterpretations is that the rule demands uniform security measures across the board and that your facility must obtain a certain level of technology to implement those measures, says **Abby Pendleton**, an attorney with Royal Oak, MI-based **Wachler & Associates.**

Though security safeguards are mandated in the privacy rule and are the focus of the security rule, there is no standard set forth (see "What The Regs Say About ... Flexibility Of Approach"). Tip: "There's no certain thing you have to do or don't have to do," Pendleton clarifies.

Caution: This can be tricky when dealing with vendors or other HIPAA "pros" who want both your time and your wallet, warn experts. "Avoid those vendors trying to sell you something for security," like locked cabinets or exorbitantly priced software, Pendleton advises.

No Technological Panaceas

Also be on the lookout for those trying to sell HIPAA in a box " those one-stop security compliance solutions that tout the ability to solve all your problems in one nice little package. "There are no easy solutions," says attorney **Alan Goldberg** of New York's **Goulston & Storrs.** That means you can't simply install some software and consider yourself compliant. "Compliance is part of a process," he reminds.

Because so many people are either smitten with or intimidated by technology, the tendency is to not question it. "The security rule is technologically neutral " there's no type of technology or brand name that is required" for compliance, Pendleton says.

What to do: You should test and retest, and really get to the heart of your compliance needs before investing your compliance future in one particular software or brand, she advises.

No Price Tags

Don't forget your budget. "Look at the cost of security safeguards versus the value of information you're protecting," and then determine your approach, Pendleton counsels.

Remember: "The security rule is really a balanced approach. Security mechanisms should never impede care," she says.

"You have to do a risk assessment to know exactly where your risks are," reminds **C. Jon Burke**, a California-based data security specialist for **Toshiba American MRI** and **Toshiba American Medical Systems.** The risk assessment will tell you where you need more security and where you are safe. However, -"you can't blow anything off and assume it's safe," Burke cautions.

"There's a knee-jerk 'this is the least of my problems' reaction" to some security worries, Burke says. However, you cannot determine that something isn't a problem until you've performed a risk assessment. After that you can determine if you need to budget for a particular security measure or if it truly is something you can afford to leave alone, he stresses.

The good news: "The security rules do allow organizations to take budget and size into account and are written to be flexible," Pendleton counsels. Keep in mind: Budget and size must be offset by level of risk.

No Set Log Lengths

Another common and equally erroneous belief is that all entities should be approaching audit trails the same way. Again, with the security rule's flexibility and your entity's size and budget, this kind of standardization is preposterous, experts say.

"People are making auditing harder than they need to," says **Kerry Kearney**, a partner at **Reed Smith** in Pittsburgh. Strategy: The key to understanding the auditing requirement is to learn two things: whether you are a target and who is after you.

"If you're securing a hospital with great risk," then you know you have to make your security foolproof, Burke clarifies. This is because any facility's "biggest threat comes from inside. It's almost always an employee with access," he warns.

Tip: Because your greatest threat is not outside attack, you can cater your audit trails to parallel your susceptibility. "Extensive heavy-duty auditing will pick up any espionage that exists, but how many of us are really espionage targets?" Burke asks.

Answer that question and then decide whether you need an extensive audit system that will detail every hit and every miss your systems receive in a day, he says. "Before auditing can work, organizations have to have a good idea what they're looking for," and without a good risk assessment that's impossible, Burke states.

No Need To Track Everyone

Example: "We've had fights with covered entities who wanted every individual employee of a business associate who logged on to have a separate ID," Kearney says. This insistence that entities track every user down to contractors or other independent employees is excessive, she notes.

"There's nothing in the regulation that says any individual person working with the business associate has to be identifiable at every log in," Kearney asserts. **Planning:** Rather than overextending yourself (and your budget), your facility should demand that business associates have an internal tracking system of who has accessed PHI, she recommends.

"It's perfectly fine to have the business associate produce its own record of who those employees were" if there's ever an inspection, Kearney counsels. Tip: This will reduce your organization's security rule implementation load and allow you to focus on other security safeguards within your entity, she says.