Health Information Compliance Alert

SECURITY: 5 EASY WAYS YOU CAN BATTEN DOWN YOUR WORKSTATIONS' HATCHES

Experts reveal how to protect your computers and keep security rule violations at bay

Even the most advanced internal security controls won't mean a thing if you haven't secured your organization's computers from external threats. Here's help you can put to good use now to keep your workstations - and your patients' PHI - out of the wrong hands.

1. LOCK UP YOUR HARDWARE

The simplest way to ensure no one tampers with your organization's computers is also the easiest: "Close your doors and lock them" when you are at work and when you step away from your computer, recommends **Rick Ensenbach**, senior security consultant with Shavlik Technologies in Roseville, MN.

Not only will this keep people from walking in and seeing what you're looking at, it will also protect any confidential information you've got lying on your desk, Ensenbach notes.

Tip: Thwart hardware thieves by asking your IT department to lock down all workstations with cables, suggests **Scott Supman**, information security director at OhioHealth in Columbus.

2. SAVE YOUR SCREENS

Even the most outdated operating systems are equipped with screensavers. For workstations that can't be turned away from public view, set the screensaver to come on after a specific period of inactivity, Ensenbach suggests. Rule of thumb: The strictest security experts call for a five-minute lapse in activity before the screensaver comes on, but if your risk assessment allows it, you can shoot for a lenient 10-minute time frame, he says.

Tip: For computers with only one user - think the billing office or reception desk - password-protect the screensaver. That way, once the screensaver comes on, no one except those with the password can access information from that workstation, explains **Shenethia Jones**, security officer for Texas Health Resources in Arlington.

Good Idea: Password-protected screensavers don't work as well in an environment where many users are sharing a station (e.g., the nurses' station or another clinical environment). Instead, try a single sign-on (SSO) method, Jones offers. With SSO, once the screensaver comes on, the original user is logged off and the next user can use her own information to access the system rather than trying to track down the first user, she says.

"We also use privacy screens in high traffic areas" where it's hard to keep PHI on the computer screen out of public sight, Jones comments. And usually priced less than $100 at any office supply store, privacy screens won't break your budget, experts assure.

3. ALWAYS LOG OUT OF YOUR SYSTEMS

"Your staff members shouldn't stay logged on to a system that accesses PHI when they're going to be away from the computer" for a while, Ensenbach says. Tip: Make sure "all users log out and shut down their computers at the end of each day," Jones adds.

Though you could set your system to automatically log users out after a certain period of inactivity, "automatic logoff could cause problems within your applications," Jones warns. For example, if you're doing something in an application that takes a little longer than the set period of inactivity, the system may not recognize it and will shut down anyway - forcing you to start over, she clarifies.

Strategy: Before you implement automatic logoffs, sit down with your tech support team and examine how the control will affect each application. If you feel automatic logoff causes more problems than it solves, then don't implement it, Jones advises.

4. DISABLE YOUR DRIVES

If you are concerned someone might make off with confidential information by saving it to a floppy disk or other removable media, you can easily turn off your computers' drives and ports, Ensenbach says.

Important: Enforce password-protected screensavers and user logoff during inactivity to avoid this measure. Then you won't need to disable a computer's drives "unless you are worried about internal threats" such as employees' inappropriate access and use of PHI, Ensenbach points out.

5. MAKE SECURITY PART OF YOUR ROUTINE

Don't just tell people what they should or shouldn't do - make security a component of your entity's culture, Ensenbach advises. Tip: Post reminders in common areas like employees' break rooms or lounges, publish reminders in newsletters or send them in a mass e-mail to all your staff members. "You could even slip something into their payroll envelopes," he offers.

Getting the message out is half the battle - getting employees to listen and care is the other half, Jones remarks. If your staff members' complaints start to pile up, remember that "they have to change the way they do business, and there is a grieving process," she says. But, once they see the benefit of the change, they are happy to help.

The Bottom Line: "You can't make [security rule compliance] sound like a business directive - it has to touch employees personally so they can make the connections," Ensenbach notes. Tip: Focus on a different security 'hot topic' each month to keep your staff energized about security, he suggests.