Codify
BY AAPC

Health Information Compliance Alert

SECURITY STRATEGIES: PROTECT PHI ON YOUR MEDICAL DEVICES WITH THESE TIPS

5 techniques to ensure your patients' PHI stays out of unauthorized users' reach

Problem: Your medical devices aren't always under your control. Just thinking about all the areas in your facility that are vulnerable to a security breach is enough to drive you crazy.

Solution: Use these professional strategies to train your staffers to protect the PHI on your medical devices-whether the machines are permanently onsite or traveling cross-country for leasing.

1. Communicate-And Coordinate Security Upgrades-With Vendors

"You don't patch your medical system the same way you would your computer systems," says **Jim Sheldon-Dean,** director of HIPAA compliance for Lewis Creek Systems in Charlotte, VT.

Instead, you should educate your employees to contact each device's manufacturer or vendor before you attempt to install any updates.

Why? "Your vendor may supply you with an update that is configured specifically for your device," Sheldon-Dean explains. Failing to apply the correctly customized patch could leave you open to security risks, he warns.

Good idea: Task your personnel with developing an open line of communication with vendors-and creating a contact list for key people at each company-so that you don't have to hunt someone down for an answer to your security questions.

Your staffers should update-and distribute-the list regularly. They should also store a master list in a location that will be easily accessible in the case of an emergency.

2. Track All Your Medical Devices

It's tough to control all the data going into and out of your medical devices. What's easier is tracking those devices themselves, insists **Greg Young**, security officer for Mammoth Lake, CA's Mammoth Hospital.

"We've begun assigning a control number to our machines that can store PHI," Young says of his hospital's policies and procedures (P&Ps). "We track the device's existence from the day it enters [the hospital] until the day it leaves or is destroyed."

That way, Young knows exactly how to handle the device if it needs to be repaired -or if it is tagged for repurposing or destruction.

Important: Be sure to include all repurposing and destruction information in your tracking system.

You can also use the tracking number to coordinate audits and investigations. And, if the Centers for Medicare & Medicaid Services ever comes knocking, you can quickly produce a history of each device, Young notes.

Action plan: Create a spreadsheet that contains all the tracking numbers you've assigned to medical devices. Then coach your staffers to update the tracking sheet when a device's stats change-or at least every six months.

Create A Separate Network For Medical Devices

Warning: Any medical device attached to your information system has the potential to blow a huge hole in your network if its security configuration differs even slightly from that of your other machines (such as laptops or handheld devices).

For example, if an MRI machine's security configuration makes it vulnerable to a certain virus-one that your desktop computers are immune to-allowing the MRI machine to share the network with your desktop computers could allow the virus to ravage your system.

Try this: Ask your tech team to develop a subsection of the network for medical devices that will isolate the devices from the rest of the network traffic, Sheldon-Dean suggests.

4. Backup All Information Stored On Your Devices

Scenario: A medical device that stores PHI breaks down. If you've not backed up that machine, you could lose all that data, Sheldon-Dean notes.

Luckily, most devices transfer the information they contain to another repository, such as patients' medical records. However, if a copy is not kept elsewhere, you must ensure that you thoroughly back up your data.

Important: You must always protect backup media, Sheldon-Dean points out. Apply the same P&Ps to that information as you do to all other data you store.

5. Beef Up Your Physical Security Measures

While technical safeguards are crucial to protecting the data stored on your medical devices, you cannot ignore your physical security measures, says Robert Markette, an attorney with Gilliland & Caudill in Indianapolis.

Explain it this way: Now that your staff recognizes medical devices as potential security risks, coach them to handle the devices the same way they do the other computers in your facility. Example: They should lock up mobile ultrasound machines just like they do laptops
.
And, if you have multiple patients using the same machine (such as a mobile unit or back-to-back X-rays), you should ensure that each patient sees only her own PHI-not the PHI of the person before or after her.

THE BOTTOM LINE

You cannot stand guard at every machine that contains patients' PHI. However, by
providing your workforce members with these simple tools, you'll help them keep your medical devices remain safe from unauthorized users.