Codify
BY AAPC

Health Information Compliance Alert

SECURITY STRATEGIES: HOW TO KEEP YOUR OUTDATED HARDWARE FROM LEAKING PHI

Use these best practices when removing health information from your office

You know your computers and storage devices won't last forever. But dumping your PHI-laden hardware could land you with a security rule violation. Try one of these media disposal techniques before your PHI trash becomes someone else's treasure.

1. KEEP PHI OFF HARD DRIVES & REMOVABLE DISKS

"Our goal is to move away from media use in any way we can," shares **Jim Donaldson**, corporate privacy and security officer for Baptist Health Care Corporation in Pensacola, FL. That means disabling floppy drives, USB ports and all other avenues for saving information off your network, he explains.

Of course, there are legitimate reasons for authorized users to save PHI to their personal workstations. For example, busy docs may store PHI on their handheld devices throughout the day.

Best practice: Your policy should determine how long PHI should remain on a staff member's hard drive - whether that's one day, one week or one month. After that, the disk must be wiped to ensure PHI isn't accidentally leaked to unauthorized viewers, Donaldson stresses.

2. ERASE ALL DATA FROM HARD DISKS & DEVICES

Whether you give your hardware to a business associate, charity or the dump, you have to ensure it's scrubbed of any lingering PHI, notes **William Hubbartt**, a health care consultant with Hubbartt & Associates in St. Charles, IL.

Best practice: Use your policy to set up a schedule for wiping hardware of stored PHI on a recurring basis. For example, because floppy disks can get worn out with heavy use - causing you possibly to lose vital information - you may decide to scrub and trash disks every 90 days. Devices with a longer shelf life - like computers and PDAs - can be evaluated annually, he notes. (For more information on data removal, check out "5 Common Methods To Give Stored PHI The Boot" later on in this issue).

3. SEPARATE SENSITIVE INFORMATION FROM REGULAR TRASH

Not all of your organization's garbage is confidential, Hubbartt acknowledges. Everyday trash like "office management paperwork, notes, memos and other documents not relevant to patient care" can be scrapped in regular waste bins.

Best practice: Lock your drives and disks containing confidential medical information in "bins that allow material in, but not out," such as those provided by shredding companies, advises **Lisa Cavitt**, information technology coordinator for Southern Illinois Healthcare in Carbondale. Tip: Make sure your CIO or security officer has a key to the bins in case the wrong information is tossed, she adds.

Tactic: "As an incentive to use the bins, we kept the disposal costs in the compliance budget and any costs associated with storing PHI were rolled back to the individual departments," Donaldson says.

4. COMPLETELY DESTROY YOUR HARDWARE

The technique that allows you to have the most fun also offers the surest guarantee that PHI will actually be rendered unusable, Donaldson says. This includes running computers through an MRI machine, smashing them with sledgehammers or using them for target practice.

Best practice: Look to shredding companies to take care of your outdated hardware if you don't have the time or resources to destroy it onsite, experts offer. Donaldson's shredders can handle all Baptist Health Care Corp's disposal needs - from paper docs to CDs to computers.