Codify
BY AAPC

Health Information Compliance Alert

Security Strategies: Don't Assume PHI Is Safe In Staffers' Homes

5 tips help you protect your patients' PHI in an unsecure environment.

It seems harmless: some at-home coding here, a little catching up on data entry from home there -- and then WHAM! You're facing a security breach. Don't wait for a disaster to strike. Use these five tips to help your employees secure PHI in their homes.

- **1. Train home workers differently than office workers.**- You have to "distinguish a data entry person who is hired to do work at home from a doctor who takes work home for the night," says attorney **Kirk Nahra,** a partner at Wiley Rein & Fielding in Washington, DC.

For employees who rarely work from home, design a procedure that requires them to go through special channels for permission. That way, you can ensure they are aware of special security precautions that they must take when PHI is removed from the controlled environment of your office.

2. Reinforce your rules with your policy.- Don't rely on training alone to enforce your rules for employees' home offices. Tip: Create a policy on how your staff should treat PHI outside of the office and have each worker sign it.

You also need a policy as to when it's OK to remove PHI from the office, Nahra says. Strategy: Design a procedure so that employees must sign out laptops for temporary home use. On the sign-out sheet, add a disclaimer that lists your staff's responsibilities and obligations to protect PHI at home. Bonus: You can use these sign-out sheets to track the flow of PCs and PHI in and out of your office.

3. Separate work computers from those used for personal activities.- You must demand that employees designate a computer for work use rather than share a workstation with their families, experts agree.

It's too risky to do work on the family PC because there's always the chance PHI could accidentally be stored on the hard drive.

If you cannot afford to supply equipment for your staffers to use at home, coach them never to store patients' information in their homes on a long-term basis, Nahra says. Example: "If you bring home reports, you should take them back; if you review something on your computer, you must ensure it's not saved to your hard drive," he offers.

4. Set the security controls on home computers to match those in the office. Any off-site computer setup must resemble your office's environment as closely as possible. If the computer is hooked into the Internet, you must "ensure you've got a good firewall so there's no way someone can get into your system," Nahra counsels.

But you don't have to buy a firewall for each employee working at home, explains **Lee Kelly,** a senior security consultant with Fortrex Technologies in Frederick, MD. Most PCs come with a built-in firewall that you can configure to protect information without shutting down the flow of operations, he says.

5. Focus on workstations' physical security. "Anything you do in the office physically to protect PHI should also be done at home," Kelly emphasizes. This includes setting up your work area so that you minimize the risk of people

inadvertently seeing PHI.

There are several ways to avoid this type of violation. Here are some easy methods:

· Work in a low-traffic area (ideally with a door).

· Don't keep your back to passers-by.

· Password-protect your computer.

· Log out instead of leaving your PC idle.

· Set your password-protected screensaver to come on after a short period of inactivity.

· Lock diskettes and other media in a desk or cabinet.

· Shred any misprints, faxes or other PHI hard copies-that you don't need.

The bottom line: While you may choose to ban workers from leaving with PHI, some small practices can't afford not to let employees work from home. With strong policies and procedures, PHI at home won't spell disaster for your facility.