# Health Information Compliance Alert

## Compliance Strategies: Don't Monkey Around At Home With Patients' PHI

**Lax policies could throw a wrench in your HIPAA compliance plan.**

Do you allow your staff to take work home for the night or weekend? Do you outsource your patients' PHI to coders or transcribers who work from home? If you answered 'Yes' to either of these questions, you could be wreaking havoc on your HIPAA compliance efforts unwittingly. Here are some tips for securing PHI in the home.

**1. Be In The Know**

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. You must train those who are never in the office not only on how to ensure privacy, but also on how to create the type of working environment that reduces the chance of a  violation, explains **Rick Ensenbach**, senior security specialist at **Shavlik Technologies** in Roseville, MN.

For employees who rarely work from home, design a procedure that requires them to go through special channels for permission, Ensenbach suggests. 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, he says.

And don't be too quick to allow employees to take PHI home with them, Nahra stresses. You should refrain from removing PHI from your office unless it's absolutely necessary, and it should be kept at home as little as possible, he reminds.

Example: "If you bring home reports, you should take them back; if you review something on your computer, you have to make sure it's not saved to your hard drive," he offers.

**2. Polish 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, Ensenbach recommends. "In the event that something does happen, you'll have something that says, 'We did educate our people,'" he explains.

You also need a policy as to when it's okay 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. Keep 'em Separated**

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, Ensenbach says, because there's always the chance confidential information could accidentally be downloaded and stored on the hard drive. "Once PHI is on the home computer, who knows who could see it," he stresses.

And even if family members or visitors never view that PHI, an offsite staff member could accidentally expose confidential information if you ever dispose of or otherwise repurpose the PC, Ensenbach warns.

**Strategy:** Find room in your budget to purchase a few laptops for employees to use on a temporary basis, Ensenbach suggests. You can better control PHI if it is only accessed from a computer that you own, he explains. When an employee returns the mobile station, you can wipe any stored PHI off the hard drive.

**Bonus:** You can also use this as an opportunity to update any security patches or virus protection, he notes.

### 4. Batten The Hatches

Any 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 **Robert Markette**, an attorney with **Gilliland & Caudill** in Indianapolis. Most PCs come with a built-in firewall that you can configure to protect information without shutting down the flow of operations, he says. "This is useful for places where there's no central firewall," he adds.

### 5. Pay Attention To The Physical

"Anything you do in the office to physically protect PHI should also be done at home," Ensenbach 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, Ensenbach says. Here are some easy methods:

- Work in a low-traffic area (ideally with a door), and don't keep your back to passers-by.
- Password-protect your computer so that no one can simply turn it on to access your files.
- Log out instead of leaving your PC idle.
- Password-protect your screen saver and set it to come on after a short period of inactivity.
- Lock thumb drives and other storage 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 employee's work from home," Ensenbach notes. To avoid needless violations, help your workers replicate your office at home as best they can, Nahra advises. With strong policies and procedures, PHI at home won't spell disaster for your facility, he adds.