Health Information Compliance Alert

SECURITY STRATEGIES: MAKE YOUR STAFFERS' HANDHELD TOYS 'HIPAA-COMPATIBLE'

3 key steps will help you form your PDA policy

Does your staff want to use Palm Pilots, Blackberries or any of the numerous other handheld devices to get their jobs done? If you answered 'Yes,' you have to find a way to keep track of those devices before you lose control of your hardware - or your patients' PHI. **Eli's** experts have some advice to get you started.

Choose Your Devices

Before you approach employees who've expressed an interest in using a portable digital assistant (PDA), you have to decide what types of minicomputers you are comfortable with, says **C. Jon Burke**, a security specialist with Toshiba America Medical Systems in California.

Handhelds offer a variety of methods for sending and receiving information, ranging from broadcast to direct communication. Example: Some handheld devices send a signal that goes out in all directions at the same time, like yelling "Hello" across a room, Burke explains. Others are quieter - "they whisper directly in the ear of their destination," he adds. You must decide whether those loud devices are too risky for your security capabilities, he says.

Remember: If your personnel are using sophisticated PDAs, ask your IT staff to "ban the devices from connecting to your network or disable their ability to store information," counsels **Greg Young**, Information Security Officer at Mammoth Hospital in Mammoth Lakes, CA. That might be easier than keeping up with what staffers are bringing into your organization each morning, he says.

Identify Your Players

"You have to know who's using these devices to track them," notes **Robert Markette**, an attorney with Indianapolis' Gilliland & Caudill. Otherwise, you can't train your handheld users on how secure the devices, he says.

Tell your employees to come to you when they want to start using a PDA, Markette suggests. That way, you can make sure they read and understand your policy and procedure on using portable devices in the workplace.

Tip: Answer any questions your staff members have and then ask them to sign an acknowledgement that they know what their obligations are, he advises. "Keep that form for your records as evidence that the staffer was clear on what you expect," he adds.

Be firm with your policy and procedure, Young warns. If your staff bucks against your rules, "tell them - 'If we can't control how you use your PDA then you can't use it' and stand by that," he recommends.

Track While You Train

You have to teach your workforce how to secure both their device and any sensitive information you allow them to store on it, experts point out. Have your training attendees list what type of device they want to use and what they will use it for on your training forms, Markette suggests. Those forms turn into both tracking sheets and evidence of your attempts to control handhelds in your organization, he notes.

Offer this training cyclically and as employees express their desires to use handheld devices at work, Markette counsels. Good idea: Train your staffers to come to you before they get rid of or upgrade their PDAs so you can dispose of any sensitive information before the device changes hands, Burke suggests.

The Bottom Line

You have to know which minicomputers are coming through your doors, especially when they're in the hands of employees who have access to confidential information, Young points out. And by staying vigilant, "you'll keep your staff on their toes because they know they won't fly under your radar," he adds.