Codify
BY AAPC

# Health Information Compliance Alert

## Compliance Strategies: 6 Proven Methods Can Plug Portable Devices' Security Gaps

**Find out how to keep your organization's data safe from unauthorized users.**

It can happen in a second: Your employee sets her PDA down and turns to speak with someone. When she turns back to her device, it's nowhere to be found.

In the worst-case scenario, all the information your staff member was carrying around on her handheld -- including patients' PHI -- is completely open to the thief.

But you can avoid the worst-case scenario with a few simple tweaks to your security procedures for protecting handheld devices.

**1. Categorize Your Devices**

You must decide which machines you'll cover in your handheld device policy, says Rick Ensenbach, senior security consultant with Shavlik Technologies in Roseville, MN.

For example, most organizations group PDAs, Palm Pilots, Blackberries and laptops into the "handheld" category. However, there is a growing trend to throw cell phones into this category, also. "Smart phones are capable of storing all kinds of confidential information," Ensenbach explains.

**2. Map Your Mobile Device Users**

No policy or procedure will be effective if you've not pinned down exactly who in your facility is using handheld devices, notes **Elizabeth Temple**, compliance officer for Tucson, AZ's Pima County Integrated Health System.

And once you track who is using these devices, you must be sure they are the only ones using them. For instance, a staff member may want to share her device with a family member, or two nurses may swap the company laptop even though only one of the nurses is supposed to be using the machine.

**Action plan:** Establish a training session for securely using mobile devices. At the end of the session, ask staffers to jot down what devices they use to perform their job duties and then use that list to kick off your tracking process.

**3. Understand All Your Features**

Default settings could either leave your organization wide open to data hijackers or lock it down so tightly the device performs poorly. Your first move when you introduce a handheld unit to your network is to go setting-by-setting through the device's operating system to ensure that the features used are those your organization needs, Ensenbach recommends.

**Important:** "You must deactivate any feature that broadcasts your device to others or that accepts information from an unauthorized device without your knowledge or permission," Ensenbach emphasizes. After you complete this process, instruct your staffers never to fiddle with their devices' activated features without the permission of your technology team.

**4. Shorten Inactivity Periods**

A long period of inactivity before your device locks itself could be the perfect opportunity for a crook to plumb your

personnel's files. Avert this threat by demanding that your staff members set short inactivity periods, such as a one- or two-minute time lapse before the system locks down.

**5. Use Smart Password Programs**

A robust password comprised of a combination of uppercase and lowercase letters, numbers and special characters (e.g., Dh@1) will deter would-be thieves from snatching information from your staff members' handheld units.

**Great idea:** "The best and newest handhelds allow you to designate a couple key clicks as a 'quick entry' password," says David Kirby, president of Kirby Information Management Consulting in Raleigh, NC. This code allows you to avoid using your full password -- but you only get a few chances to enter the short cut code before you'll enter the full password.

A shortcut password could be highly effective because it will make staff members more likely to create complex passwords, Kirby advises. "In the PC world, staff members tend to log on and stay logged on for a very long period of time; in the handheld world, they tend to use the device a hundred times per day for 30 seconds each time," he explains.

Entering a complex password a hundred times each day is tough - and people work around it by making simple pass codes. However, with the 'quick entry' feature, easy-to-remember key clicks allow users to avoid entering that password each time. Layered security measure: If the user fails to enter the correct clicks, she must then enter the full password.

**6. Invest In Encryption**

Your personnel should encrypt any external sites such as memory cards or PC-based databases that you use to store information created or managed on their portable devices, Kirby counsels. However, encrypting the handheld devices could severely affect their performance, he says.

**Best:** Encrypt only your password-management utility on the handheld device itself. Then set your device to "self-destruct" by wiping out its memory after a certain number of attempts to crack its password, Kirby suggests.

**Crucial:** For this strategy to work, staffers must regularly synchronize their devices and backup all files so that you can replace the information the devices contain. Good idea: Swap out two or three memory cards each day so that no one card contains your entire storage content.

**Remember:** You do not need to ask employees to invest a lot of time and money into encryption. "Evaluate the risk that someone wants the device for the data it contains," Kirby advises.

If the risk is extremely high, strong encryption is a good choice ��" but the more likely outcome of that assessment is that thieves are after the device, not the information stored on it.