Adopting an eight-step approach to securing your mobile devices can help protect your data.

Your workforce is mobile, but are your employees equipped to deal with security threats that might be lurking? Computers on wheels (COWs), notebooks, personal digital assistants (PDAs), BlackBerrys, smart phones and Microsoft Windows mobile devices have a unique set of security requirements.

Mobile devices themselves — and the healthcare data contained on them — are invaluable and have five main vulnerabilities: loss, wireless network security, Bluetooth security (or lack thereof), Denial of Service (DoS) attacks and viruses.

**Loss:** The biggest security issue surrounding mobile devices is loss of the device. According to *The Washington Post*, 160,000 portable devices are left in Chicago taxicabs each year. This statistic doesn’t even include the number of portable devices that are stolen.

Mobile devices are a tempting target for theft. Steven Hughes, an engineer with the Veterans Affairs Medical Center in Boston, says, “We have COWs that run almost like terminal services, so they don’t have any patient information installed on them. If someone moves one of those [COWs] out, it would not have patient information on it.”

**Wireless network security:** Most mobile devices will use wireless fidelity to connect to the network. Out of the box, these Wi-Fi networks are either not secured or use Wired Equivalent Privacy (WEP) for security. Neil Buckley, network security manager for Partners HealthCare System, located in Boston, states, “The WEP protocol, for obvious and documented reasons, is flawed. Its encryption implementation is flawed. And WEP, as a protocol, is not capable of being managed at the enterprise level.”

When a member of your workforce is traveling with a mobile device, it’s tempting to use Wi-Fi hotspots. But data transmitted from a Wi-Fi hotspot is always available to other devices at that hotspot.

**Bluetooth security:** “Devices come with Bluetooth nowadays, but turn it off if you’re not using it,” says John Kuo, IT security engineer for Fred Hutchinson Cancer Research Center in Seattle, WA. “Those [Bluetooth devices] are really easily sniffed out.”

“Bluesniping” is a technique used to identify and communicate with Bluetooth devices at a range of up to one mile. The attacker can access e-mail messages, text messages, contact lists and calendars on the target mobile device. Sophisticated attacks could even give the hacker access to the network to which the mobile device is connected.

**DoS attacks:** In the healthcare industry, DoS is a big concern. Your mobile devices can negatively affect or be negatively affected by another mobile device. If that other mobile device happens to be a wireless medication...
pump, a DoS attack can have fatal consequences if the patient doesn’t receive the correct dose of medication.

**Viruses:** Mobile device viruses and e-mail viruses pose as much of a threat to mobile devices as they do to hardwired computers on your network. Mobile viruses can jeopardize the security of data or disable the mobile device.

**Eight Steps You Can Take to Secure Your Mobile Devices**

**Create a mobile device security policy:** Mobile devices need to be included in your existing network security policies. If you already have a policy for notebook computers, copy it and replace “notebook computer” with the mobile device of your choice. If you’re creating these policies now, here are some things to consider:

- Require a password to log on to the mobile device. Put rules in place to guarantee a strong password. If someone then gets his or her hands on one of your mobile devices, he or she may decide to reformat the device but won’t be able to recover any sensitive data.

- Have a policy that requires data stored on removable media to be encrypted. This includes secure digital (SD) cards, mini SD cards and Universal Serial Bus (USB) storage devices, as well as traditional storage media.

- Encrypt all data on your mobile devices. Better yet, don’t store any sensitive data on the device.

**Provide user education:** User education can go a long way to prevent loss. Fred Hutchinson Cancer Research Center’s Kuo adds, “A lot of it is common sense. For example, if you’re at a conference and you’re using a laptop, don’t just leave it on a table. Carry it with you whenever possible.” In addition, train users to use cable locks to secure their notebooks. Tell users not to carry their notebooks in attractive cases; instead, have them use notebook sleeves, backpacks and nondescript cases.

Train users not to save passwords when logging on to the Internet and your secure sites. Rick Hampton, wireless communications manager for Partners HealthCare System, notes, “We do look at a lot of different potential vectors. Some of them just are not addressable now with technology. You have to just rely on your staff and on your policies.”

**Use remote wipe:** Many e-mail systems now support remote wipe. This allows the network administrator to remotely format a mobile device if it’s lost or stolen. Remote wipe resets the device to its factory settings. Even so, it’s important to remember that data on removable storage should always be encrypted. Remote wipes will wipe out the data on the mobile device, but they won’t wipe out data that is on removable storage, such as a mini SD card.

**Require a secure encrypted network:** Make sure you use Wi-Fi Protected Access (WPA) to encrypt and secure your Wi-Fi network. WPA is much more secure than WEP. A determined intruder will be able to break into a WEP-protected network.

Make sure that you’re not broadcasting your service set identifier (SSID), but don’t think of this as a fail-safe solution. The SSID is part of all network communication between the device and the network. Anyone sniffing the network will be able to see the SSID rather easily.

Require that external users access your network by using an encrypted Virtual Private Network (VPN) tunnel. This is especially important if people are using Wi-Fi hotspots. Because all communication through this tunnel is encrypted, anyone else using the Wi-Fi hotspot won’t be able to see sensitive information.

**Turn Bluetooth off:** Turn Bluetooth off if it isn’t needed. Otherwise, turn off any Bluetooth services that aren’t needed.

**Use virus and spam protection:** Just because you’re using a mobile device doesn’t mean that it can’t get viruses like any other operating system. Make sure that you install virus protection software and antispam software that will work with your mobile device. This will prevent mobile and e-mail viruses.

**Use an Intrusion Detection System (IDS) and network monitoring:** Make sure to protect your network by using an IDS and network monitoring tools that are designed to work in the healthcare industry.

**Plan for data backup and recovery:** An important part of any security plan is a good system for backup and recovery. Because the only totally secure device is one that is locked in a room and not on a network, the final part of any security implementation is the ability to restore any compromised system or device quickly.

**Minimize the Risks**

Mobile devices are now part of the networks and should be treated similarly to how any computer on the network is treated. Being aware that mobile devices come with their unique set of security issues is important to designing and deploying a secure mobile device environment. By being knowledgeable and following best practices, you can minimize the risks to your healthcare organization.

---

### Mobile Device Security Checklist

Make sure you have everything you need to keep your mobile device secure.

- User education
- Mobile device wiping
- Secure encrypted network
- Turn Bluetooth off
- Virus and spam protection
- IDS and network monitoring
- Data backup and recovery strategy