Health Information Compliance Alert

COMPLIANCE TIPS: CUT THE CORD ON YOUR WIRELESS PATIENT ACCESS CONCERNS

You can allow patients to use a wireless connection without ruining your compliance program

Any time a patient connects to the Internet wirelessly from your facility, your patients' confidential health information is on the line, right? Not necessarily.

With this four-step plan, your workforce members can allow business visitors, patients and their guests to surf the Web without jeopardizing your security compliance efforts.

1: GIVE PATIENTS A SEPARATE ACCESS PATH

To protect your confidential information, tell your technology team to direct your non-employee wireless users' access to a separate channel that's isolated from your facility's network, counsels **Matt Johnson**, a HIPAA security consultant with Fresno, CA's AltaPacific Technology Group.

Your tech staff should "route all patients' access right to the Internet without bringing them near your firewall," explains **Fernando Pedroza**, director of technology and security for Poudre Valley Health System in Fort Collins, CO. This way, you both protect your PHI and maintain tight control over the chance that someone will illegally access PHI, he says.

Tip: Purchase a separate DSL connection from any Internet service provider, Johnson recommends. "Having a separate Internet connection is no different than if the building next door has an Internet connection," he notes. Next step: Teach your staff members how to use that connection so they can guide patients through the process. Good idea: You could also post a step-by-step log-on procedure in public areas for patients to use.

Important: No matter how you configure your patients' wireless access, be sure that it does not interfere with clinical use. Why? "Even if your clinical applications are not currently wireless, they probably will be in the future," explains **Matt Simon**, Manager of Security & Client Services for Emory Healthcare in Atlanta.

2: USE A PORTAL FOR TERMS OF USE

You should also "filter patients' access through a captive portal that automatically redirects the Web browser to a specific page regardless of where the user wants to go," Johnson suggests. Your portal can outline the exact terms and conditions of using your facility's computers and wireless network.

Important: Your workforce members must understand your portal's terms and conditions so they can answer patients' questions. Try this: Create a list of the terms and conditions along with an example of each one. Then give that list to your staffers to refer to if a patient is concerned.

For example, one term of use could be that the user cannot participate in malicious activity (like identity theft); another might be that the user cannot allow unauthorized individuals to use the service (like another person in the waiting area). Once the guest clicks through the portal, they are bound to abide by the terms or face consequences.

3: KEEP YOUR WIRELESS SIGNAL WEAK

Though it may seem like a strong wireless signal is ideal for patient use, you must make sure your signal goes no further

than your facility, Simon says. Patients may want to use their PDAs or laptops in the public areas outside your organization, but that's risky.

Explain it this way: Wireless networks are like radio stations. If you set the power too high, the broadcast can be heard for miles - eliminating any security measure you've implemented. Rather, "you should dial down the power so the signal is barely powerful enough to reach your outer walls - making it highly secure," Johnson advises.

Training tip: Be sure to tell your workforce members that no one should be able to access the wireless network from outside the organization. Your security policy should tell them whom to contact if they are suspicious that someone might be tapping into the network from somewhere outside the facility.

4: AUDIT ALL WIRELESS ACTIVITY

Even the most stringent security measures can be thwarted. Coach your tech team to pay close attention to what patients are doing once they get online, Simon encourages. That way, you can spot any loopholes or security gaps a savvy guest may have found.

And regular auditing will help you determine if patients are abusing your services. You may either decide to scale back their wireless access or use a content monitor like Vericept (www.vericept.com) or Vontu (www.vontu.com). Example: You could install a tool that will sort Web sites into two categories: "appropriate" (like shopping) and "inappropriate" (like gambling).

Tip: Some hospitals issue laptops and other portable devices for use within their facility. That way, they can allow "low-tech" patient and families to access the Internet, and they can control the machines to make sure that they are clear of malicious viruses and spyware.

The Bottom Line: As always, you must document both how you set up wireless access for your patients and any adjustments you make to that network after the fact, Simon says. Don't be afraid to retool the process as times goes on, he stresses. A major component of a tight security system is constant evaluation and improvement.