Health Information Compliance Alert

Technology Training: Warn Your Staffers About This Wireless Technology Trap

Physician groups and other rogue access points could destroy your compliance efforts.

If you don't clamp down on who can access your wireless network, you leave it wide open for unauthorized users -- including people who stumble onto it accidentally.

"A large problem right now is physicians' offices or other groups piggybacking on the wireless network of a hospital that shares the same space" such as in a medical plaza, says **Tom Walsh** of **Tom Walsh Consulting** in Overland Park, KS. If the separate group can jump onto your wireless router, you'd better believe a criminal can.

Your best strategy for avoiding this problem is to control your wireless access points -- the spots in your organization that allow users to connect to your router. Use this professional guidance to keep your wireless network safe from opportunists and crooks alike:

• **Match up MAC addresses:** "Set up your wireless router so that it only accepts traffic from specific Machine Access Code (MAC) addresses," Walsh suggests. That forces any computers attempting to connect to the router to present the address like an ID, he explains.

Important: You must supply the MAC address for each device on your wireless network, including any that your staffers bring in, such as laptops or PDAs. And, any remote workers must configure their wireless networks the same way, or users can jump on their routers to access your network, Walsh says.

• **Ask for authentication:** You must make staffers sign on to your wireless network using an approved username and password, says **Chris Apgar**, CISSP, president of **Apgar & Associates** in Portland, OR. That way, someone who's hijacked a machine with the right MAC address must still work to crack your security.

• **Test for easy access:** Also called 'war driving' and 'parking lot surfing,' you must walk around your facility -- and your neighborhood -- to ensure that your wireless access signal reaches only as far as you want, and that your access controls are working, Apgar says.

Remember: You must do this at least once per year, and then more regularly as you suspect someone may be inappropriately using your wireless network.

The Bottom Line: Any users who connect to your wireless network without your permission are setting you up for a security breach, experts warn. Not only will they operate in a way that's incongruent with your policies and procedures, they could also allow identity thieves to sneak in through the back door. Crack down on inappropriate access now -- before your patients' PHI falls into the wrong hands.