Health Information Compliance Alert

Case Study: Tips For Taming The Wireless Access Beast

Wireless networking isn't the technology bear it's made out to be.

That's the attitude **Fernando Pedroza** took when deciding to implement wireless access for patients, visiting physicians and staff members at the Poudre Valley Health System in Fort Collins, CO.

"We were getting a lot of requests from physicians who wanted access to different systems and applications, so we decided to allow everyone access to the Internet," rather than loading the requested information on all the system's PCs, Pedroza explains.

Pedroza then set up the following access levels to ensure that no one can view or manipulate confidential information without the correct authentication information:

Level 1: **Patients and visitors only.** Non-employees who want to use the Internet are allowed to use their own computers. However, they do not have the ability to choose their destination. Rather, the system is set up to shuttle them directly to a public Web site.

Level 2: **Regular workforce members.** Staff members are issued devices that are configured to connect directly to an encrypted network. They are still required to authenticate to the network using a strong password.

If a staffer attempts to access Poudre Valley Health System's encrypted network using a personal device, he or she will only be allowed to connect to the Internet.

Level 3: **Visiting physicians and other caregivers.** Part-time physicians and nurses are assigned a username and password. They then access patients' information through a Virtual Private Network. This allows them to use the organization's applications without sacrificing any security measures, Pedroza explains.