InfoWorld

STRATEGIES & TACTICS

Wireless health driven by HIPAA

By Eugene Grygo April 05, 2002

CONFORMING TO THE federal government's HIPAA (Health Insurance Portability and Accountability Act) regulations regarding patients' security and privacy has put Concentra Health Services, an Addison, Texas-based occupational therapy group of physicians and physical therapists, in a predicament.

As the company deploys 802.11b WLAN (wireless LAN) in Concentra's 231 clinics, executives mull over whether they should implement hardware firewalls between its many WLANs and its core network, says Jay Wilson, the company's vice president of IS and technology, and chief technologist. As are many of the HIPAA regulations, this issue is not clear cut, he says.

"Our legal and IT departments are going through and writing each of our HIPAA policies for all of the different areas that HIPAA covers," Wilson says. "We will definitely have a road map for our wireless network ... [but] HIPAA is not black and white, so it doesn't tell you exactly what the answer is."

Health care CTOs need to understand 802.11b security flaws and develop a solution with IT enhancements as well as strict policies and procedures, says Michael E. Stull, a principal at eHealthcare.net, a consultancy based in Alexandria, Va.

Users will have to master "authentication and, for example, turning on the ability of the system to use the access control lists of the MAC [media access control] address of the network card [used in] accessing the LAN," Stull says. CTOs will have to apply these controls at the network, VPN, and notebook and device, or at each level. According to Stull, the first course of action is to remove the widely publicized "default condition of 802.11b that lets anyone into the network."

Most of the mobile road map has been laid out for Concentra. The first leg of the journey was to eliminate an expensive medical transcription system that cost $3 million to $5 million. To get there, Concentra's IT staff developed its ChartSource application and deployed the Roam About Wireless access point system from Rochester, N.H.-based Enterasys Networks.

"We wanted an application that could be taken with the provider -- the physician -- into the exam room ... . It was a lot less expensive for us. Instead of putting a device in every single exam room, we just have to have one device per physician, and they can wander from exam room to exam room. That was the driving force behind putting in a wireless network," Wilson says.

Concentra's programmers spent about five months building ChartSource with Microsoft Visual Studio using Visual Basic script, Microsoft's COM (Component Object Model) objects, and XML and XSL style sheets.

The point-and-click application allows a physician to click on a patient's name to display his or her medical history. After an examination, the doctor feeds the diagnosis into ChartSource as well as "the completed and signed medical note and puts it back into our Practice Management System [database]," Wilson explains. The customized system includes a decision-tree application for consistency in patient reports.

ChartSource is supported via Enterasys hardware, including the wireless access card on each handheld device. The medical information is forwarded to a centralized datacenter where a WAN links the clinics to a another datacenter. ChartSource runs under Citrix Systems' remote application management software, which passes the screenshot, keystroke, and other thin-client information back and forth. "All the heavy processing is done on the server farm that's located here in Texas," Wilson says.

Concentra's IT staff has completed the second phase, a pilot program with its physical therapists, and a third phase governing patient check-outs and care-giver billing is in the works. "We are integrating the handheld with our internal prescription-dispensing system," Wilson adds.

Deployment for 1,000 physicians and physical therapists underscores how good a match wireless and medicine make, Wilson says. For now, Concentra's WLANs are HIPAA-compliant. Wilson wonders if WLANs will require stronger security measures.

CTOs' options may increase as WLAN technology evolves, vendors and industry observers predict. Aside from firewalls, IT staff will have to implement a layered approach to WLAN security, involving authentication and periodic dynamic key exchange, analysts say. CTOs will need to consider third-party tools that authenticate wireless users rather than relying on WEP (Wireless Equipment Protocol) keys, according to Stull.

"Security is a very holistic thing," advises Kelly Kanellakis, general manager of Enterasys' Roam About offerings. "For security to be implemented well, you really need to take a layered approach ... . The higher your risks are, the higher the cost of a breach in security, then you need to look at more security measures."

Eugene Grygo is a writer based in New York.