



January 1, 2007

Wireless health center secured

Software thwarts hackers while addressing regulatory compliance issues.

In 1999, the University of Utah Health Sciences Center (UUHSC) deployed an office-wide Wi-Fi network, to be used by healthcare providers to better serve their patients. Instead of relying on wired connections, providers would now be able to remotely check medical records, reports and images, as well as the vital signs of their patients. This led to greater mobility in the clinical environment and more rapid access to vital information whenever or wherever a healthcare provider might be.

Since then, UUHSC has grown into one of the largest employers in Utah, with more than 9,000 employees, and the wireless network has undergone a metamorphosis of its own. Although the network started as a way for healthcare providers to wirelessly access critical patient data, the network was subsequently opened up to the wider community. Now, researchers, students and even patients are able to use the wireless network. With so many users, and so much sensitive, personal information being sent through the airwaves, the IT team at UUHSC began to feel the need for a comprehensive security solution in order to protect patients' records and other sensitive information.

While attending a network security seminar, UUHSC information security analysts saw a demonstration showing how a wireless network signal could be extended by thousands of feet using a single potato chip can as an antenna. This was an eye-opening moment for the team, which now realized the threat it was up against, and how simple it could be for outsiders to gain access to a wireless network. The UUHSC team decided it was time to find a way to secure the ever-growing wireless network in order to prevent a breach.

Adding to the urgency of the situation, UUHSC is legally mandated by the Health Insurance Portability and Accountability Act (HIPAA) to enact security measures to protect "electronic personal health information." Healthcare providers access sensitive medical information about their patients on a daily basis on the wireless network, and although no breaches had occurred in the past, the possibility of a security breach on the network can never be ruled out. Without a multilayered approach to security in place, patients' records could be transmitted in clear text where anyone could potentially snatch them from the air, violating patient privacy and the government mandate that UUHSC protect this information.

Originally founded as a single hospital in 1965, UUHSC is now made up of a network of community clinics, academic colleges, and various institutes and centers. The organization offers clinical services to patients across a broad network of centers in Utah

and the intermountain region, as well as education and research programs for individuals in the medical field.

Bo Mendenhall, principal information security analyst at UUHSC, knew that proactive steps needed to be taken in order to protect the data being sent out over the network. “Our primary responsibility on the security side is to maintain the confidentiality of our patients’ information,” he says. “In order to stay ahead of the curve, we started searching for a security solution that could monitor our entire network and keep hackers’ hands off the confidential information being accessed by our users.”

When considering security options for wireless networks, organizations in the healthcare industry must go above and beyond the normal protocol in order to protect their patients’ personal information. In addition to being unlawful, not securing sensitive information in the clinical setting can be bad for business. If patient data were to be stolen due to poor network security, the healthcare facility would stand to lose consumer trust and would be in jeopardy of serious financial ramifications. UUHSC was mindful of these considerations, and opted to beef up its wireless network security before a problem presented itself.

UUHSC sought a solution that would protect the information on its network without affecting the availability or integrity of the data, since it was critical that healthcare providers had access when they needed it. Mendenhall and his team sought a comprehensive solution that would allow them to track and easily discover rogue access points. In addition, the solution would need to track and shut out hackers from the network.

Mendenhall and his team previewed several security solutions, deciding that a sensor-based solution would be optimal. After testing several options, UUHSC opted for AirDefense’s Enterprise offering. “We were drawn to the comprehensive features of the solution,” offers Mendenhall. “Compared to the other offerings on the market, it was easy to use and administer, and could be accessed from almost any machine with a browser.”

AirDefense Enterprise is a sensor-based solution that allows IT teams to monitor both security and performance on an organization’s wireless network. Using these sensors, UUHSC is able to locate rogue access points with precision and block them before they are able to threaten the wireless network. The security setup is also able to recognize unauthorized users and block them from gaining access to the network, ensuring that only UUHSC personnel and authorized guests are using the wireless LAN.

In addition, AirDefense Enterprise 7.0 includes many features that were particularly useful in the clinical environment. The solution provides HIPAA compliance documentation, audit trails of alarm events and response to ensure proper enforcement of privacy policies—a sanctioned HIPAA requirement.

“It’s more important than ever for organizations to secure their wireless networks in addition to their wired ones,” Mendenhall says. “We’re constantly trying to stay ahead of

the hackers, and in addition to our AirDefense solution we also have wireless policies and guidelines in place that employees are required to follow. Educating individuals who use wireless networks is another essential layer in the overall security of the network.”

While implementing security solutions is an important part of the wireless network puzzle, Mendenhall explains, education is an integral part in keeping information secure. Users must be aware of the existence of rogue access points, which may appear to be valid access points to an unsuspecting employee logging onto UUHSC’s network. When users are alert and aware of the potential security risks of using a wireless network, hackers are only put at a further disadvantage.

“In our case, implementing a multilayered security platform has given us peace of mind, knowing intruders will be shut out of our network and patient information is well-protected,” Mendenhall says.

For more information from AirDefense:
www.rsleads.com/701cn-253