



“AirTight gives us a way to envelop our infrastructure with comprehensive protection.”

Dana Seflow, director of information technology, SynergyHealth



## AirTight is the Right Prescription for SynergyHealth to Safeguard Electronic Medical Records

### The Challenge

Following the deployment of a wireless network that would be used to access electronic medical records, improve internal communications, and provide patients and visitors a way to check e-mail and surf the Web, SynergyHealth needed a way to ensure that the infrastructure was both highly available and secure. AirTight’s SpectraGuard was the prescription.

SynergyHealth—Leading the way to improved services through technology

If you need medical care in Wisconsin’s greater Washington County area, you’re more than likely to turn to SynergyHealth. SynergyHealth is a regional health system that includes an 80-bed acute care hospital built in 2005, six clinics throughout the county, an eight-bed residential hospice, cancer care, surgery, and outpatient rehab centers.

As part of its mission to improve the quality and accessibility of health care, SynergyHealth leverages technological advancements fully to further the progress of patient care. That aim includes the use of electronic medical records so that clinical information is made available wherever practitioners may be. But the security and accuracy of those records is critical.

“With the move to electronic medical records, we must make sure doctors and nurses have the tools to access that information throughout the campus—whether it’s checking patient data before entering a room, or administering medication at the bedside,” says Dana Seflow, director of information technology for SynergyHealth.

Such ubiquitous access is made possible through the recent installation of a Wireless Local Area Network (WLAN), 130 Workstations on Wheels (WOWs) and 110 WiFi phones for the network. As part of the move toward wireless networking, SynergyHealth also made available a wireless hotspot to give visitors and patients access to the Internet and their e-mail.

### OVERVIEW

#### SynergyHealth Organization:

Provides Wisconsin’s greater Washington County area with an 80-bed acute care hospital, multiple medical clinics, an eight-bed residential hospice, and cancer care, surgery, and outpatient rehab centers. St. Joseph’s Hospital, West Bend Clinic, and SynergyHealth Foundation are members of SynergyHealth.

○ **Business Problem:** As the health system relied increasingly on electronic medical records and wireless network access, the provider needed to find a manageable, cost-effective way to secure its growing wireless infrastructure.

○ **Operational Challenge:** Standard encryption protocols don’t provide the security SynergyHealth could trust. And manual wireless security would be unwieldy. SynergyHealth sought an automated wireless intrusion prevention system that was easy to deploy and manage, and was highly accurate.

○ **Solution:** AirTight Networks’ SpectraGuard

#### ABOUT AIRTIGHT NETWORKS

AirTight Networks is the industry standard for wireless vulnerability management and the only company that offers a flexible, end-to-end solution that gives customers visibility into their wireless security posture and a choice in how they manage it. AirTight's SpectraGuard Enterprise provides a robust wireless intrusion prevention system (WIPS). Its SpectraGuard Online service is the world's first on demand wireless vulnerability management service which provides a flexible approach to addressing wireless vulnerabilities with no capital investment. AirTight's patented technology delivers the key elements of an effective WIPS to eliminate false alarms, block wireless threats immediately and automatically and locate wireless devices and events with pinpoint precision. AirTight's customers include global retail, financial services, corporate, education and government organizations. AirTight Networks is a privately held company based in Mountain View, CA. For more information please visit [www.airtightnetworks.net](http://www.airtightnetworks.net)

## The Problem—Standard Wireless Encryption Protocols Do not Deliver Security

While the move toward wireless access to electronic medical records promises improved efficiencies and instant access to information, SynergyHealth also had to make certain that the WLAN was highly available, secured from potential eavesdroppers, and complied consistently with the security and privacy rules of the Health Information Portability and Accountability Act (HIPAA). And, considering all of the recent news surrounding the ease with which wireless networks and encryption protocols can be broken, the organization wanted to make certain its network wasn't vulnerable.

"I don't care what wireless encryption you use, all of them are crackable," says Seflow. "We knew early on that we'd need more robust security than the standard protocols."

While encryption protocols add some level of security to network traffic when in transit, they do nothing to detect and protect the network from rogue access points, users intentionally—or unintentionally—accessing unsecured neighboring networks, or a host of other attacks to which WLANs are susceptible. The IT team had considered using Network Address Translation (NAT) to limit access to the network but, with so many devices, that proved not only complicated but also time consuming and difficult to manage continuously.

Additionally, while the first wireless networks would be deployed primarily in rural areas, future WLAN deployments would take place in more populated urban settings, so the healthcare provider wanted to make sure that its users couldn't accidentally connect to neighboring networks, which would create an obvious security risk.

"We didn't want to place ourselves in a situation of constantly reacting to all of these issues. We wanted to have manageable, proactive security in place," says Seflow.

**"We had to be absolutely certain they [WiFi-enabled patients and visitors] couldn't access the wireless network with sensitive patient data. SpectraGuard gives us that level of certainty."**

—Dana Seflow, director of information technology, SynergyHealth

## The Solution—Attaining a "Comprehensive Envelope" of Protection

Following a careful market evaluation, SynergyHealth opted to deploy the SpectraGuard® Wireless Intrusion Prevention System (WIPS) from AirTight Networks. SpectraGuard proved to be the perfect way to keep the WLAN secure, segregate public WiFi access, and help to assure regulatory compliance. SpectraGuard provides rogue AP and client detection, prevents accidental and risky connections to neighboring WLANs, and constantly monitors wireless traffic to identify and defend against potential attacks.

“AirTight not only makes certain that we’re secure, but also keep us from having to constantly patch and update the latest encryption schemes,” says Seflow. “AirTight gives us a way to envelop our infrastructure with comprehensive protection.”

The SpectraGuard architecture, which typically consists of a server and wireless sensor devices, scans the airways continuously and provides automatic protection against unauthorized wireless activities, access, and rogue traffic—without ever disrupting authorized wireless communication.

“SpectraGuard was very easy to install, and AirTight’s service team did a great job helping us to bring the system into production,” says Seflow.

Shortly after completing the initial deployment, SynergyHealth conducted an assessment to confirm that SpectraGuard was operating as it should, and that the WLAN was secure. “The system was working flawlessly,” says Seflow. “That was great news.”

While that level of protection is crucial for any organization, it’s especially so for a hospital with a public hotspot designated for patients and visitors.

“Because we are a public building, anyone can be here and legitimately use the hotspot. That makes it even more challenging to be sure that our primary network is secure,” Seflow says. “We had to be absolutely certain they [WiFi-enabled patients and visitors] couldn’t access the wireless network with sensitive patient data. SpectraGuard gives us that level of certainty.”

Moving forward, Seflow appreciates how SpectraGuard not only will keep the WLAN secure, but also ease—through comprehensive reporting—regulatory compliance efforts.

“We’ll now have real-time alerts and periodic reports that will detail any deviations from security and regulatory policies. Such insight will help demonstrate our regulatory compliance quickly. That’s very powerful.”

Now, with SpectraGuard in place and fully protecting SynergyHealth’s primary WLAN, SynergyHealth will soon extend the benefits of tether-less access to electronic health records to many of its other locations. Seflow says it “We’re going to expand these efforts and we’ll all sleep better—knowing that we’re able to identify and block any potential security breaches.”

### Wireless Vulnerability Management

AirTight Networks, Inc. 339 N. Bernardo Avenue #200, Mountain View, CA 94043  
T +1.877.424.7844 T 650.961.1111 F 650.961.1169 [www.airtightnetworks.net](http://www.airtightnetworks.net) [info@airtightnetworks.net](mailto:info@airtightnetworks.net)

© 2008 AirTight Networks, Inc. All rights reserved. AirTight Networks and the AirTight Networks logo are trademarks, and AirTight and SpectraGuard are registered trademarks of AirTight Networks, Inc. All other trademarks mentioned herein are properties of their respective owners. Specifications are subject to change without notice.

