

HIPAA Compliance for Healthcare WLANs

Healthcare professionals are rapidly discovering the advantages and criticality of wireless LAN (WLAN) solutions in their organizations. The unparalleled freedom offered by wireless networking provide hospital personnel with mobile, real-time access to the information and applications they require to better serve patient requirements, especially at the point-of-care. In today's world, IEEE 802.11-based WLANs enable healthcare providers to use a variety of mobile computing devices (laptops, PDA's or tablet PCs) to securely exchange vital yet sensitive information such as medical records, lab results, prescriptions for medication, electronic imaging and admissions data. Healthcare WLANs can deliver clear benefits such as:

- improved patient care
- enhanced administrative and care provider productivity
- minimize transcription and prescription errors
- expedited transaction processing
- stronger inventory controls

However to realize such impressive benefits, numerous wireless security and management challenges must be successfully addressed to realize these benefits.

WLAN security and management issues are not simply technical problems that must be resolved. How healthcare organizations address these issues can have a clear impact on the ability to derive business and medical value, and on regulatory requirements such as the Health Insurance Portability & Accountability Act (HIPAA).

WLANs and HIPAA Requirements

HIPAA privacy rules require a healthcare organization to define and implement policies, procedures and other measures to ensure that only authorized individuals have access to patient health information. Typically hospitals, healthcare providers, and insurance companies are affected by HIPAA. Specifically, HIPAA calls for organization-wide security measures for, "protecting data as it is accessed and as it travels anywhere throughout the participating organizations." There are five main requirements for compliance with HIPAA security standards for electronic patient medical data:

- Confidentiality. Ensure that patient medical information is not made available or disclosed to unauthorized individuals.
- Integrity. Ensure that data has not been tampered with en route or in storage.
- Authentication. Verify that only authorized users can access the network and that the person transmitting data is who he or she claims to be.
- Authorization. Allow authenticated users access to network resources and data based on defined permissions
- Non-repudiation. Once a transaction occurs, neither the sender nor the recipient can deny that it took place.

Organizations subject to HIPAA must also provide audit trails for access to patient medical data: who accessed the file, when they accessed it and for what purpose they accessed it. **Under HIPAA, WLANs are considered "open networks" that require the implementation of mechanisms to ensure access control (authentication and authorization) and over-the-air security.** Thus, deploying WLANs in healthcare organizations present specific HIPAA compliance

"There isn't much point in having a secure wireless network if it is not usable. As an example, we evaluated VPNs for the WLAN and concluded that the security advantages were outweighed by the fact that it made the network much harder to use and even harder to manage. Roving Planet gave us a solution that delivered everything we need for security and enhanced HIPAA compliance while also making the WLAN easier to use and manage," said Randy Nale, IT Manager at St. Francis Medical Center in Louisiana.

"Protecting data as it is accessed and transported is key to HIPAA compliancy."

Complete mobility created by wireless LANs fundamentally changes the requirements of wireless systems management. By using the Roving Planet CSD, healthcare providers can solve some of the pressing issues common to a variety of hospital and healthcare wireless LAN environments:

- **Reduce the cost of deploying wireless infrastructure**
With the Central Site Director, a single wireless network can provide many different users and user groups access to a range of applications such as computerized physician order entry, electronic prescribing, patient records, high-speed Internet access and VoIP telephony.
- **Enhance wireless LAN security**
Central Site Director provides dynamic firewall capabilities at each access point, enabling control of access to particular applications based on user, time, and location or specific access point.
- **Reduce wireless LAN management costs and service bottlenecks**
Central Site Director's real-time network monitoring, historical reporting, and distributed administration features ease the central administrative burden, help maximize capacity utilization, and enable rapid identification and isolation of network issues. Additionally, CSD provides automated bandwidth throttling at each access point to ensure service levels for applications and users.
- **Enhance wireless LAN control, uptime, and management flexibility**
Central Site Director lets administrators easily restrict all access, or limit access to certain resources, in specific access points or locations at specific times. Furthermore, CSD enables run-time addition, deletion, and updating of applications, users, and user groups, and also provides run-time dynamic management within individual and across multiple VLANs and SSIDs.
- **Investment protection**
Central Site Director leverages currently installed wired and wireless infrastructure, supports a variety wireless hardware vendors, and guarantees wireless LAN performance as the complexity of the application environment grows.

"The Roving Planet CSD provides us with the means to easily and securely provision access for various types of guests and internal users while also providing us with the detailed visibility that we need in order to know what is happening with our wireless network and our users, applications and devices," said Randy Nale, Manager of IS Technical Services.