



HIPAA Compliance and Wi-Fi™

NETWORKS

October, 2005

**XIRRUS**

Introduction

The popularity of in-building wireless or Wi-Fi™ networks continues its rapid growth across multiple industries. Within the Healthcare industry, wireless applications such as electronic prescriptions, electronic lab work requests, results retrieval, wireless admissions processing and wireless asset control are allowing institutions to improve accuracy and efficiency. However, in order for these organizations to make use of Wi-Fi technology, the solution must allow them to comply with the Health Insurance Portability and Accountability Act (HIPAA). This document looks at the requirements for wireless networks to comply with HIPAA and how the Xirrus Wireless LAN Array makes it easy to implement and comply with those requirements.

HIPAA Background

The Health Insurance Portability and Accountability Act (HIPAA) was passed by the US Congress in 1996. The regulation calls for the privacy and security of patient information. Compliance further requires that network controls be enacted to protect sensitive communications that are transmitted over open or private networks so that the communication cannot be easily intercepted by anyone other than the intended recipient. Wireless networking falls into this category.

HIPAA does not address the extent to which a particular entity should implement the specific features. In fact, there is no official HIPAA certification program; instead, HIPAA requires that each affected entity assess its own security needs and risks and devise, implement, and maintain appropriate security measures to address its business requirements. Within the regulation, high level areas are outlined for the healthcare organization to address and are listed below.



Unique identification
and authentication
of users



Only authorized
access to critical
business assets



Levels of
access control



Secure (encrypted)
communication



Auditability of
all records and
access logs

In order to comply with the regulation, an organization's wireless solution must provide multiple levels of security to address each of these concerns.

Securing Patient Data

To ensure that only authorized personnel can read and manipulate data; the wireless system must include a method of uniquely identifying wireless users, and authenticating their identity. One method to handle secure authentication is through the use of the IEEE 802.1x specification for authentication, or more commonly implemented using a RADIUS server.

In addition to authentication, only those users authorized to use a specific network or system should have access to it. Network device administration must also be controlled so that device settings can only be changed by network administrators. Additionally, the solution should authenticate all the pieces of the wireless network infrastructure to prevent unauthorized network intrusion through unauthorized wireless access points.

Different levels of access control allow administrators to define who is allowed on the network and which network resources they have available to them. These mechanisms assure that people have access only to the information they need to do their specific function.

As data travels from a wireless device to the organization's network, anyone can intercept the data and possibly even tamper with it. To assure that only intended parties have access to the data, encryption schemes must be employed in data transmission. In addition, data integrity must be verified by the recipient. The strongest encryption scheme that accomplishes this requirement is WPA (Wi-Fi™ Protected Access) with AES (Advanced Encryption Standard). By using this, health care facilities can assure that no one can intercept or manipulate user data transferred over the wireless network.

The final piece that a HIPAA compliant wireless system must address is event logging and alarm reporting. By tracking who accesses the network and which resources are accessed, auditors must have records to trace transactions. In addition, by alerting system administrators of possible network attacks, administrators are better able to track and mitigate any possible compromise of the network.

Xirrus Provides HIPAA Compliant Wi-Fi™

The Xirrus Wireless LAN Array enables healthcare institutions to take advantage of all the benefits of a wireless network while still complying with HIPAA regulations. By integrating leading edge technologies into the Wireless LAN Array, Xirrus assures proper authentication, authorization, access control, encryption and audit controls.

The Wireless LAN Array incorporates the following features to enable organizations to address each HIPAA security requirement for wireless networking.

User Authentication

The Wireless LAN Array has complete 802.1x authentication protocol support including EAP-TLS, EAP-TTLS, or PEAP for use with external enterprise-class RADIUS servers that ensures only authorized users gain access to the wireless network.

For smaller organizations, the Xirrus WLAN Array contains an integrated RADIUS server for use with up to 1024 users which eliminates the cost and administration of an external RADIUS server.

Secure Wireless Connections

The Wireless LAN Array supports strong, government-grade wireless data encryption standards including Wi-Fi™ Protected access with both TKIP and AES-CCM that eliminates any eavesdropping of wireless packets.

Access Control

Levels of access control for users can be implemented by defining which Wi-Fi™ networks each user is allowed to connect to. Administrators can also define which VLANs are assigned to each wireless network such that physical network separation is achieved for specific network resources. This can restrict user access to specific portion of the network.

Intrusion Detection and Prevention

The Wireless LAN Array contains a dedicated Integrated Access Point Radio to continuously monitor and alert the presence of an unauthorized “rogue” access points or unauthorized client station on the wireless network.

The MAC address of lost or stolen laptops can be entered into a special list that will block access for those devices and create an alert to the fact that attempts to access the network are being done with those devices.

Additionally, the use of the Xirrus XM-3300 Central Management System will alert the presence of other types of wireless security issues including denial of service attacks, man-in-the-middle attacks, the presence of peer-to-peer wireless networks and other issues. The Xirrus Central Management System can automatically trace these security issues on both the wired and wireless side of the network and automatically contain or eliminate such threats.

Each Wireless LAN Array is authenticated with the Xirrus XM-3300 Central Management System ensuring that only authorized devices are apart of the trusted wireless network infrastructure.

Secure Administration

The Xirrus solution provides for secure administration of the wireless network. All management interfaces are secured with multi-level password protected administrative accounts and assignable privileges.

Secure management over the network is done through secure protocols such as secure http (https), secure shell (SSH) and SNMP V3.

Additionally, the use of the Xirrus XM-3300 Centralized Management System, default policies can be created such that newly deployed Wireless LAN Arrays are automatically configured in compliance with security policies.

Audit Controls

Detailed logs that capture the “who what and when” is accessing the wireless network along with other security threat alerts are captured on each Wireless LAN Array.

These event logs from each Xirrus Array can be forwarded to an existing enterprise Syslog server, or aggregated to the Xirrus Central Management System. Logs can then be reviewed and should be part of a periodic compliance audit.

Configuration change audits allow administrators to view changes made to each Xirrus array.

Summary

The Xirrus Wireless LAN Array provides the needed features of user identification, authentication, access control, secure management, encrypted wireless transmissions, automatic intrusion prevention and automatic audit controls for HIPAA compliance.

By integrating all the features into the Xirrus Array needed to address the elements defined in the HIPAA regulation, the Xirrus WLAN Array enables any organization to comply with the federal requirements in an easy and automatic manner.

The Xirrus Wireless LAN Array

Xirrus has delivered on a new class of product called a Wireless LAN Array. By solving the fundamental problem of allowing multiple access points to function at very close proximity to each other in a single platform, Xirrus has created a new paradigm for high-performance Wi-Fi deployments. This new architecture allows Xirrus to provide nearly a Gigabit of wireless bandwidth over a large coverage area. The Wireless LAN Array eliminates the capacity bottleneck with fifteen times the capacity of other access points— all in a single platform. No longer will Wi-Fi deployments require a sea of access points to be deployed, managed and serviced. Today's bandwidth hungry applications such as Voice over Wireless LAN are now handled with ease, and the costs of the wireless network are substantially reduced in a healthcare environment.

Xirrus offers a complete family of Wireless LAN Arrays differentiated by the number of Integrated Access Points (16, 8, 4) supporting a variety of healthcare deployment types. The XS-3900 Wireless LAN Array integrates 16 Integrated Access Points with a high gain, Multi-sector Antenna System to provide 864Mbps of Wi-Fi bandwidth over a coverage area that is typically four times that of a typical access point. This unique, multi-radio, multi-sector design simultaneously uses up to 15 non-overlapping channels to maximize the RF bandwidth available within a given coverage area.

Each Wireless LAN Array also provides a dedicated Integrated Access Point for monitoring and reporting of the RF environment for exceptions such as rogue access points greatly increasing the security of the Wi-Fi network and protecting patient information. Through a partnership with AirMagnet, Xirrus has embedded AirMagnet's award winning sensor software within the Wireless LAN Array offering healthcare institutions a complete Wi-Fi network that provides high performance connectivity and dedicated Intrusion Detection and Prevention without the need of a separate overlay sensor network.

The Array Architecture allows up to twelve 802.11a and 4 802.11a/b/g Integrated Access Points in the same device. The Integrated Access Points are arranged in a circular configuration (much like the numbers on a face of a wall clock). The Array Controller is at the heart of the Array Architecture and provides advanced radio intelligence and system management allowing the Integrated Access Points to work in a coordinated fashion. The Multi-sector Antenna System provides increased directional transmit Gain (clients in one direction can hear the WLAN Array more clearly) and provides increased receive gain (allows the WLAN Array to hear clients more clearly from one direction). The result is a coverage pattern that increases rate, range, and capacity in all directions. For more information visit www.xirrus.com.

About Xirrus

Xirrus, Inc. is lead by Dirk Gates, former Chairman and CEO of Xircom. The Company has assembled a team of professionals successful in developing Enterprise-class mobility and wireless products. The Company has technical and management expertise gathered from developing both client and infrastructure products at leading companies such as Airgo Networks, Alcatel, Allegro, Calix Networks, Extreme Networks, Intel, Nomadix, Practical Peripherals/Hayes, Xircom and Zhone Technologies. ●



Xirrus, Inc.
370 North Westlake Blvd.
Suite 200
Westlake Village
California 91362
805.497.0955 Corporate Office
805.497.0955 x300 Sales
805.449.1180 Fax
www.xirrus.com

Copyright 2005 Xirrus, Inc. All Rights Reserved. The Xirrus logo is a registered trademark of Xirrus, Inc. All other trademarks and registered trademarks are the property of their respective owners. Content subject to change without notice.
October 2005