

Wireless LANs and Healthcare: Understanding Security to Ensure Compliance with HIPAA

Healthcare is a natural environment for wireless LAN solutions. With a large mobile population of doctors, nurses, physician's assistants and other caregivers, wireless LANs bring the ability to access the latest patient charts, medical records and clinical decision support data at all times, anywhere in the healthcare organization. And as caregivers travel among different facilities, wireless allows for easy connectivity at each site. Early adopters in healthcare recognized these benefits and deployed the first wireless LAN solutions in the late 1990's.

However, with wireless LANs comes a new security risk. Unlike wired networks where physical access is required, wireless LANs transmit signals into the air space, and can extend beyond the physical perimeter of rooms and buildings. The standards which wireless LANs are based on, IEEE 802.11, does not mandate over-the-air security and authentication of users. Unless specifically configured for security, most wireless LAN equipment is an 'open' network, or able to be attached to by any wireless LAN client. This obviously could lead to serious security risks if unauthorized personnel were to gain access to the healthcare network.

While security vulnerabilities endanger the integrity of any corporate network, the risks are magnified in healthcare due to HIPAA legislative requirements. HIPAA, or the Healthcare Information Portability and Accountability Act, is a law passed in 1996 by the US government that aims to simplify the processing and distribution of medical information, improve the portability of health insurance, give patients access to medical information and protect patient data that is stored, transmitted or accessed across networks. The HIPAA scope is large and many resources are available to help healthcare organizations with understanding its wide ranging implications. The applicable section for wireless LANs is *"Security and Electronic Signature Standards - Section 4. Technical Security Mechanisms to Guard Against Unauthorized Data that is Transmitted over a Communications Network."*¹ Specifically, this section of the HIPAA guidelines requires:

¹ The complete HIPAA standard can be found at <http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-3877.pdf>

HIPAA Standards	Sections	Implementation Specifications (R) = Required, (A) = Addressable	
Access Controls	164.312 a 1	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	164.312 b		(R)
Integrity	164.312 c 1	Mechanism to authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	164.312 d		(R)
Transmission Security	164.312 e 1	Integrity Controls	(A)
		Encryption	(A)

Recommendations for Wireless LAN Capabilities to Meet HIPAA Standards

To meet HIPAA guidelines, the Meru Wireless LAN System delivers the following security features:

WPA Encryption and Authentication

WEP-based security has been proven to be easily cracked and therefore is insufficient to meet today's enterprise security requirements. It also doesn't provide for authentication between the client and the network. To solve this problem, the Wi-Fi Alliance created WPA, an industry standard for strong over-the-air encryption (TKIP) coupled with mutual authentication between the client and the network based on IEEE 802.1x. The Meru Wireless LAN System is Wi-Fi Alliance Certified™ for WPA. In addition, Meru also allows creation of Access Control Lists based on MAC addresses to provide an additional layer of security.

Proven Interoperability with a WPA-compliant RADIUS Server

RADIUS servers such as Cisco ACS, Funk Software Odyssey and Meetinghouse AEGIS provide the back-end authorization capabilities for users trying to access the wireless network. RADIUS servers provide mutual authentication to defeat rogue servers. When used with EAP-PEAP or EAP-TTLS, a secure channel is established through which the end user's identify and password-based credentials are passed during authentication. This provides security against dictionary attacks while leveraging

standard user name and password infrastructure. Authentication and dynamic per-session keys can be generated at any interval to encrypt the wireless connection, minimizing the weaknesses of WEP and protecting against man-in-the-middle or hijacking-session attacks.

RADIUS servers also should support RADIUS Accounting which provides IT managers with an audit trail for network access. Information regarding the date, time and credentials is stored at log-in and log-out. Multiple unsuccessful log-in attempts may also be logged. The Meru Wireless LAN System is fully compatible with a wide range of popular RADIUS servers.

Support for Multiple VLANs with Independent Security Settings

Many different types of users may need to access the healthcare wireless LAN network. Doctors, nurses and other caregivers need access to patient records, charts and test results. Other staff such as dieticians and medical billing staff don't need access to sensitive patient data. Virtual LANS (VLANS) allow each authorized wireless LAN user to gain access to only the network resources they need to see. In addition, healthcare institutions often use barcode scanners for inventory, supply or patient tracking. These types of devices often do not support today's more advanced WPA security, but the less secure WEP encryption. They too can be segregated on a specific VLAN which only allows access to the specific database or application they are associated with. This, along with frequent encryption key changes and MAC address control lists, mitigates potential security risks. The Meru Wireless LAN System supports up to 64 independent VLANs (based on SSID) with different security settings per access point. Each SSID can be mapped to a specific VLAN port, providing enhanced security by restricting network resources based on user type and application.

Addressing Security Management, Configuration and Incident Reporting Procedures

Beyond protecting the wireless LAN itself against vulnerabilities by using WPA for strong encryption and authentication, the HIPAA standard also requires that certain administrative and procedural controls be in place to protect the security and integrity of the data. Because wireless has become so ubiquitous, new risks to the institution are inherent due to wireless client mis-association, ad hoc networks and mis-configured access points. In this area, the HIPAA standard requires that:

HIPAA Standards	Sections	Implementation Specifications (R) = Required, (A) = Addressable	
Security Management	164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)

To address these issues, the Meru Wireless LAN System provides the following capabilities:

Defense Against Rogue Access Points

With the ready availability of inexpensive consumer-grade access points, a new threat has emerged to enterprise security. Employees with a desire to have wireless connectivity, may bring access points into the enterprise and plug them into the corporate network, without any security mechanism enabled. Once behind the firewall, anyone within range of the signal can connect and access the network or do malicious hacking. Proactive rogue access point detection ensures that the enterprise is protected from this threat. The Meru Wireless LAN System proactively searches out rogue access points. Through scanning of all 2.4 and 5 GHz channels, the Meru Wireless LAN System can identify unknown and non-authorized access points, alerting IT administrators. Clients attempting to associate with a rogue access point can be automatically blocked, preventing all access to the Enterprise network unless through an authorized access point.

Notification of Configuration Changes

Mis-configured access points can lead to unauthorized users accessing the network, or private healthcare information being broadcast in the open for others to eavesdrop. The Meru Wireless LAN System integrated with security partners like AirDefense provides the ability to constantly monitor the access points and ensure that all authorized access point security policies remain in place. If the access point configuration changes, immediate notification is provided to the IT administrator and all client connections to the mis-configured access point are prevented.

Prevention of Additional Internal Security Violations

Beyond rogue access points, the most common threat to the corporate network security is formation of ad hoc networks, or authorized wireless clients connecting to neighboring wired networks. In both cases, this can leave the healthcare institution open to security violations as confidential healthcare information may be accessed on the client device through these insecure and unauthorized connections. The Meru Wireless LAN System integrated with security partners like AirDefense continually monitors the airwaves throughout the enterprise for internal security violations such as these, and automatically prevents them before confidential information can be transmitted.

Incident Reporting Procedures

Malicious acts are also a possible occurrence in today's environment. Man-in-the-middle attacks, reconnaissance (i.e. use of NetStumbler) or denial of service attacks are all possible threats to the healthcare network. The Meru Wireless LAN System integrated with security partners like AirDefense immediately detects these threats and prevents them. In addition, all security violations whether malicious or not, are logged and reported to the IT administrator via email, pager or cell phone. Response to these events is also tracked to maintain an audit trail of the timeliness of the resolution.

Summary

The Meru Wireless LAN System provides a wide range of security options and controls to ensure healthcare institutions are HIPAA-compliant. A wireless LAN network can be implemented with confidence, allowing the institution to reap the enormous benefits of a converged voice and data wireless LAN.

Access Controls (Section 164.312a1)

- Unique User Identification: Username and password through WPA-based IEEE 802.1x authentication. Can be supplemented with MAC Address Access Control Lists for additional control.
- Encryption and Decryption: TKIP. Dynamic re-keying via WPA-capable RADIUS server.

Audit Controls (Section 164.312b)

- Via SNMP through WPA-compliant RADIUS server.

Integrity (Section 164.312c1)

- TKIP implements a Message Integrity Check to ensure data has not been compromised.

Person or Entity Authentication (Section 164.312d)

- Using WPA with 802.1x authentication, each user must enter a unique user name and password to gain access to the network.

Transmission Security

- Integrity Controls: TKIP implements a Message Integrity Check to ensure data has not been compromised.
- Encryption: TKIP encryption. Dynamic re-keying via WPA-capable RADIUS server.

Security Management (Section 164.308a1)

- Risk Analysis: Continuous monitoring of air waves for security violations including rogue access points, ad hoc stations, improper configurations, accidental associations. Provides a continuous review of security policy and vulnerability assessment of the wireless LAN.
- Risk Management: Implementation of a 24 x 7 wireless monitoring system mitigates potential risks due to wireless threats.

Incident Reporting Procedures (Section 164.308a6)

- Immediate detection of intruders with alerts to security managers of type of event, time and event resolution.