AN AIRMAGNET TECHNICAL WHITE PAPER

Wi-Fi, Health Care, and HIPAA

WLAN Management in the Modern Hospital

by Wade Williamson

WWW.AIRMAGNET.COM

Table of Contents

The Wi-Fi Opportunity

Wireless networking has quickly become a critical aspect of daily life in the hospital IT environment. With the maturation of the 802.11 standards (collectively known as Wi-Fi), hospital staff can remain connected to their critical systems regardless of their location in a facility. Additionally, a new breed of mobile applications has evolved that provide care-givers and administrators with on-demand access to the information and systems they need to better serve their patients. This has led to an increase both in the accuracy and efficiency of hospital operations, which has in turn led to patients that are more satisfied and better served. Typical Wi-Fi enabled applications in health care include:

Electronic Prescriptions - Physicians can electronically issue prescriptions while on rounds - immediately sending the prescription to the patient's pharmacy while automatically checking for known allergies and conflicting medications. This improves accuracy and safety while streamlining paperwork.

Lab Work/Results - Physicians can electronically order detailed tests for their patients and securely view results as soon as they are available.

Admissions - The wireless network has allowed hospitals to overhaul and streamline the patient admissions process. Instead of holding incoming patients in crowded waiting areas, they can go straight to a personal room where they are individually admitted by staff equipped with mobile PCs.

Hospital Administration and Management - Hospital administrators can see the latest up-to-the-minute information on all of their key assets and programs. Supplies can be scanned and tracked, and patient information can be entered directly into the system once, instead copying information between multiple forms.

Before hospital staff can put their trust into a wireless network, IT must know without a doubt that the WLAN is secure, performing at a high level, and reliable in even the most challenging environments. These requirements not only make sense from a technical standpoint, but are also federally mandated by the 1996 HIPAA regulations. This paper examines these security and performance requirements, and shows how AirMagnet provides IT with the visibility and control needed to address these challenges.

Security

Security typically tops the list of concerns when deploying any wireless LAN, and hospitals are certainly no exception. Patient information is some of the most sensitive data to traverse any network, and federal HIPAA guidelines have established sweeping standards dictating how this data should be protected. While these guidelines allow each organization to choose the technology best suited for their unique needs, they are explicit as to what standards of quality these solutions should meet.

Technical Safeguards

The "Technical Safeguards" section of the HIPAA standard establishes five core security concepts that address the overall protection of patient data. They are:

1. Access Control
2. Audit Control
3. Data Integrity
4. Entity/Person Authentication
5. Transmission Security

Of these requirements, Transmission Security has direct relevance to wireless networking, as it explicitly addresses how information should be treated while transmitted over an "open network". Specifically, it states that data must be encrypted while on an open network, and ideally would include some mechanism to check the integrity of the transmitted data.

Functionally, these requirements mirror standard network security directives that messages should only be “readable” by the intended recipient(s) and that the recipient should be able to verify that the data hasn’t been modified in transit. The final version of the HIPAA rules make integrity checking optional and the requirement can be met with any solution that employs standard checksum functions. These functions are common to most modern encryption strategies, thus leaving health care IT with several options when selecting their encryption strategy. Table 1 below shows some of the strengths and weaknesses of the most common security strategies used in WLANs today.

Regardless of the security solution chosen, IT must be able to verify that all users and infrastructure in the network actually use the prescribed security at all times. This means being able to track the security of every access point and client in the environment. Without this visibility there is no way to know whether the formal security policy “on paper’ is actually being practiced in the field. AirMagnet provides exactly this function; allowing IT to set the security policy of their choice and monitor that policy on every device in the network. This allows IT to see any rogue devices in the network, and identifies APs or clients that are putting the security of the network at risk. AirMagnet can immediately raise an alarm when a device deviates from the security policy, and the offending device tracked down with a mobile version of the AirMagnet network analyzer.

Security Management Process

Strong security deployment is not simply the result of implementing a security protocol or feature, but an ongoing process that continually assesses the network

for evolving threats and vulnerabilities. The HIPAA standard, to its credit, identifies this fact and sets forth a comprehensive management process that covers:

Prevention - Prevention entails a programmatic approach to vulnerability assessment to identify any potential weaknesses in the security deployment before they can be exploited. This is an ongoing process and is often under-addressed.

Detection - Security management systems depend upon quick accurate detection of violations in the network. Without it, Containment and Correction are just not possible.

Containment - Once a violation is detected, technical staff need enough specific information to pin down the source of the violation in order to limit the scope of the violation.

Correction - Correction requires the combination of event specific data with up-to-date industry best practices in order to mitigate a threat and prevent a recurrence.

Table 1. Security Types

Security Type	Strengths	Weaknesses
WEP	• Near ubiquitous support in all Wi-Fi hardware • Provides encryption for traffic on the WLAN	• Well documented attacks to break the encryption mechanisms • Single-sided authentication opens the door to MAC spoofing and Man-in-the-Middle Attacks

802.1x with LEAP	• More secure through use of rotating keys • Much more resistant to Spoofing and Man in the Middle Attacks	• Requires users to remember a Password • Password subject to Dictionary attacks
802.1x with TLS	Very Secure	• Requires each user to have a certificate
VPN	Very Secure	• Requires software on each client • Lowers performance/throughput

At the heart of every AirMagnet solution is a dedicated analysis engine designed to automate these steps into one seamless management process. This engine (AirWISE) constantly analyzes the wireless network for over 40 unique security vulnerabilities and attacks, allowing technical staff to see issues as they evolve and to respond before a security violation occurs.

Furthermore, AirMagnet alarms gives the information and advice needed for IT to respond. Each alarm singles out the devices (down to the MAC address) and/or channels involved, accompanied by a detailed explanation of what the alarm means, why it is important, and even suggests best practices that could resolve the problem. This capability ties prevention, detection, and response into one unified process that the network team can act on.

Tracking and Documentation

The final piece of the security management process is to document incidents in the network in order to provide an ongoing view of network security issues. This logic dictates that it is not enough simply to say the WLAN is secure - instead, the security process must be verifiable and auditable. To this end, the HIPPA standard requires the ability to perform “an internal audit, which would be an in-house review of the records of system activity”. This provides for two important things. First, the ability to track security issues over time provides staff with the empirical evidence and logic for how the security policy should be modified in response to real-world events. Second, a strong documentation process provides the proof needed to show compliance during an audit or legal action. In the end, this proof of security can be almost as valuable as the security itself.

Table 2. Security Summary

HIPAA Requirement	The Solution	What AirMagnet Provides
All patient data must retain privacy and integrity. This includes: • Data Integrity • User Authentication • Transmission Security	Patient data must be protected by encryption with user authentication. Typical options include: • WEP • 802.1x with LEAP • VPN • TKIP/MIC	Regardless of which encryption is used, IT must ensure that every Access Point and Client in the network actually uses that security in order for patient data to remain protected. AirMagnet automatically monitors every device to insure it is running the security of your choice, and will raise an alarm if any device breaks from the policy. As a result, you can be sure your security policies are enforced and all patient data is encrypted while on the WLAN.

HIPAA Requirement	The Solution	What AirMagnet Provides
The solution must be able to detect security violations and regularly assess for new weaknesses	24x7 Network Monitoring and Intrusion Detection	AirMagnet Distributed provides a 24x7 vulnerability assessment, identifying over 40 specific security problems including intrusions such as Rogue devices, MAC address spoofing and a variety of DoS Attacks.
The solution must include a mechanism for identifying and tracking security violations in the network	Customizable alarming and tracking	AirMagnet includes a total of 90 alarms that can be configured to the needs of any environment. Alarms detail the source of the problem, if possible down to the offending MAC address. Alarms can be saved for further analysis in the AirMagnet Management Server.
Security policies and results must be documented, tracked, and reported to verify the ongoing success of the security policy	Archiving and reporting of security issues	AirMagnet Reporter provides 50 customizable reports to show trends in the network, the history of security issues, and overall policy compliance.

To address these documentation issues, AirMagnet augments its intelligent alarming capabilities with a complete reporting solution with over 50 customizable reports. These reports allow managers to quickly see the overall health of the network in terms of security and performance, and can provide an archive of all

security incidents and violations that were detected in the network. This provides the ongoing insight needed to properly identify the dangers in a particular environment and how to evolve security policies going forward.

Table 2 provides a summary of HIPAA requirements as they apply to wireless LANs, and how AirMagnet helps to meet those requirements.

Performance

With the overwhelming industry focus placed on security, it is easy to lose sight of the importance of performance and reliability in the wireless network. The real-world fact is that even the most secure WLAN is a failure if it doesn't meet the needs of the end users. This is particularly true in a hospital environment where all systems are highly critical and users may not always have the luxury of simply plugging in to a wired network in the event that their wireless fails. Hospital WLANs in particular, have some unique characteristics that can make performance management especially challenging.

High Density of Mobile Obstacles - Medical environments are packed with devices that could potentially block or distort RF coverage, and many of these devices are moved throughout the day. This could include medical equipment or something as straight-forward as stainless steel carts used to carry supplies.

Shielded Rooms - X-ray rooms are lead shielded for obvious safety reasons. However, since these rooms will block RF signals as well, they can create coverage "shadows" for the WLAN.

Many Sources of Interference - With such a high density of technical devices, there is an increased potential for unintended electromagnetic interference in the Wi-Fi spectrum. Given that these devices may be only used intermittently, being able to detect bursts of noise in real-time is critical to identifying the source.

Highly Mobile Users - Users of the WLAN will roam from location to location far more regularly than in a typical office environment. IT needs the ability to see how the movement of users is affecting the network, and to see if concentrations of users are overloading the wireless infrastructure.

Performance Monitoring Needs

To properly address these challenges, IT needs a system that delivers as much performance intelligence as it does security intelligence. In addition to providing complete visibility, the solution must automatically identify the underlying cause of performance and reliability issues, and then provide the tools needed to test and pinpoint problems in the network. This should include the ability to:

Identify Known Trouble Spots - IT must have the tools to identify areas that have poor signal strength, poor signal quality due to multi-path, or poor data rates. This will allow IT to decide whether existing infrastructure can be modified to provide better coverage or whether the area may warrant its own access point. The AirMagnet Mobile Suite offers tools to perform detailed site surveys, coverage tests, and signal quality tests to identify these trouble spots while the network is being deployed.

Monitor All Resources - IT needs to quickly see if infrastructure is being overburdened, including the utilization and throughput on a per channel basis, and which clients are using which resources. AirMagnet provides this ability to inspect the network by channel and infrastructure to see instantly how all assets are being utilized.

Automated Root Cause Analysis - Performance management should be proactive. This requires a dedicated analysis that can identify the root causes of problems and not simply report on the symptoms of a problem. AirMagnet solutions automatically detect 45 performance and diagnostic issues that can lead to problems in the network. Each issue can generate a detailed alarm which includes best practices for responding to the problem.

Mobile Tools - In addition to monitoring, IT needs tools they can use in the field to pinpoint the cause of problems and actually get them resolved. AirMagnet includes a battery of tools built for this purpose. Tools include a connection troubleshooting tool, AP performance tools, signal quality tool, coverage tool, as well as traditional tools such as Ping, traceroute, whois, and more.

4x7 Proactive Monitoring - As Wi-Fi has matured, it has become one of the more critical pieces of IT infrastructure in the modern hospital. Like any critical system, WLANs are judged in terms of down-time, and require monitoring that can identify problems regardless of when and where they occur. Network administrators need real-time visibility into all of their wireless assets with the ability to see developing problems before they can lead to a service outage.

Table 3. Performance Summary

Requirement for Robust Network Performance	What AirMagnet Provides
Determine the best placement for Access Points, identify coverage "dead-spots"	AirMagnet Mobile solutions include a detailed Site Survey utility to determine the ideal configuration of your wireless network, and proactively identify trouble-spots. An additional Coverage Tool lets you measure all areas of your network against service levels that you set, so that you can insure performance standards in the WLAN.
Detect Noise and Interference	AirMagnet automatically detects environmental noise or interference between devices in the network and raises alarms in response.
Detect Overloaded Devices and Channels	Wireless infrastructure can support only so many users and/or traffic. AirMagnet watches over the entire wireless infrastructure and can raise alarms when any one piece of the network is overburdened. Thresholds can be tuned so that IT can respond before users are impacted.
Monitor Channel Utilization and Throughput	AirMagnet provides insight into how each channel is using its available resources, allowing IT to diagnose the health of each channel in real-time. Troubleshooting Tools
Troubleshooting Tools	AirMagnet's Mobile solutions include tools that IT can use to determine the source of connection problems, identify malfunctioning access points, and much much more.

The combination of HIPAA regulations and the critical nature of hospital applications has made wireless LAN management one of the top issues facing health care IT organizations. AirMagnet solutions have been specifically designed to meet these challenges, and provide technical teams with the systems and tools needed stay in control of their networks today and into the future.

About AirMagnet, Inc.

Founded in 2001, AirMagnet, Inc. provides the most trusted WLAN management and security software systems for the enterprise in handheld, laptop and distributed configurations. Used by IT professionals at more than 2,600 companies worldwide in manufacturing, financial, retail, service, health care, utility, transportation, education and government sectors, AirMagnet solves Wi-Fi connection problems, tracks down unauthorized access, simplifies site surveys, and locks in unprecedented levels of network performance, security and reliability. Additional information about AirMagnet and its products is available on the Web at www.AirMagnet.com.