AirTight NETWORKS

Wireless Security and Healthcare – Going Beyond IEEE 802.11i to Truly Ensure HIPAA Compliance

339 N. Bernardo Avenue, Suite 200 • Mountain View, CA 94043
www.airtightnetworks.net

AIR COVER FOR NETWORK SECURITY

Wireless Security and Healthcare –
Going Beyond IEEE 802.11i to Truly Ensure HIPAA Compliance

Wireless LANs are prevalent in healthcare institutions. The constant need for mobility among doctors, nurses and staff while remaining connected to clinical information systems is a natural environment for Wi-Fi networks. And with new, innovative hands free Wi-Fi phones, use of voice clients in healthcare is also increasing, eliminating the need for noisy, overhead paging systems and the frustration of missed calls. The number of applications that Wi-Fi is used for within healthcare continues to grow, increasing the Wi-Fi network's importance as a mission critical component of the network infrastructure.

However, with wireless LANs comes a new security risk. Many healthcare IT organizations are aware of the need for properly securing the wireless LAN and using secure over-the-air encryption and authentication methods such as WPA and WPA2. However, this alone is not enough to prevent security risks. Inexpensive consumer-grade access points, typically unsecured and brought in without malice by employees, can open up the healthcare network to anyone within range of the signal.   And, Wi-Fi enabled laptops, can accidentally connect to neighboring networks, leaving the laptop open for port scanning or other malicious activity.

While serious threats endanger the integrity of any corporate network, the risks for healthcare institutions in the United States are magnified 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. Since patient data is transmitted over wired and wireless LANs, HIPAA requires that the healthcare institution take all necessary measures to prevent unauthorized access to such patient data. Moreover, if unauthorized access does occur the institution must prove that it has procedures in place to handle such security incidents.

The HIPAA scope is large and many resources are available to help healthcare organizations with understanding its wide ranging implications. The applicable section for Wi-Fi networks is "Security and Electronic Signature Standards - Section 4. Technical Security Mechanisms to Guard Against Unauthorized Data that is Transmitted over a Communications Network." Specifically, this section of the HIPAA guidelines requires:

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)

In addition, Sections 164.308(a)(1) and 164.308(a)(6) require that administrators set up a security management process and security incident procedures. These must apply to both the wireless LAN deployment as well as the wired network.

Standards	Sections	Implementation Specifications (R) = Required, (A) = Addressable	
Security Management Process	164.308a1	Risk Analysis	(R)
		Risk Management	(R)
Security Incident Procedures	164.308a6	Response and Reporting	(R)

Recommendations for Wireless LAN Configuration to Meet HIPAA Guidelines

To meet HIPAA guidelines, organizations installing a wireless LAN should look for a system that delivers the following security features:

WPA2 or WPA Security

WPA2 and WPA provide strong over-the-air encryption (AES or TKIP, respectively) coupled with mutual authentication based on IEEE 802.1x between the client and the network

Proven Interoperability with a WPA2 or 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. They also provide a method which allows for auditing the users accessing the network.

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 WPA2 or 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.

Secure Management Interfaces

The wireless LAN system should support secure, authenticated methods of management. Reconfiguring the access point through the management port is one method a malicious hacker might try to access the corporate network. Wireless LAN systems should provide SNMPv3, SSH (secure Web), and SSL (secure Telnet) interfaces. Furthermore, the system should be configurable such that management is not possible over-the-air, and ideally a management VLAN is available such that only stations on a specific VLAN can modify the WLAN network settings.

Wi-Fi Vulnerabilities Exist, Even in a 'No Wi-Fi' Organization

Despite all of the above precautions taken to secure the wireless LAN network, a serious security risk can still exist, exposing the healthcare organization to HIPAA violations. Even a "no Wi-Fi" policy is no guarantee of security against these threats. Rogue access points connected to the wired network by employees can compromise the data transmitted over wired networks. Laptops with embedded Wi-Fi can connect to neighboring networks. Both are real, significant risks.

Traditional wireline security methods such as firewalls and VPNs do not detect these types of threats. And once the device is behind the corporate firewall, it is viewed as trusted. In this new era of almost ubiquitous Wi-Fi, the corporate air space itself must be considered an asset and protected.

The eight major categories of wireless threats are described below. Each of these threat categories can lead to unauthorized access to patient data. The healthcare institution may violate HIPAA if it does not deploy systems to counter these threat categories.

Common Wireless Threats

Rogue Access Points

The most common, as well as most dangerous, wireless threat is the rogue access point. The rogue access point is typically a low cost, SOHO-class access point brought in by an employee who desires wireless access. The default access point settings typically have no security enabled, and thus when plugged into the corporate network create an entry-point for anyone with a Wi-Fi client within range.

Mis-configured Access Points

For those enterprises with a wireless LAN infrastructure, one potential threat can arise from their own equipment. An access point which becomes mis-configured can potentially open up a door to the corporate network. In particular, if the access point is reset to network defaults or the security settings are turned off. If the access point is not centrally managed, then the likelihood of it going unnoticed is high. Employees will still be able to connect so no problem will be reported.

Client Mis-associations

Embedded Wi-Fi clients in laptops are now relatively common. Even for those enterprises with a "no Wi-Fi" policy, a Windows XP laptop with a wireless client will automatically try to connect to an SSID that it has successfully connected to before. This scenario is very common for two reasons.

If the employee has connected to a Linksys, Netgear or other home or hot spot access point using the default SSID, it will automatically connect to another AP with the same SSID without the user being aware of the connection.

Secondly, neighboring Wi-Fi networks can spill into the enterprise and curious users connect to these open, insecure, and distrusted networks while still connected on the wired side of the trusted network. Users may also connect to these networks if their internal network firewall does not permit POP email accounts, does not permit access to certain web sites, or they do not want their outbound traffic monitored.

Ad Hoc Connections

Wireless clients can also create peer-to-peer connections. A peer-to-peer connection can be exploited by a malicious hacker who may try to then inflict a variety of attacks on the client such as port scanning to explore and exploit client vulnerabilities.

Malicious Wireless Threats

Evil Twin/Honey Pot Access Points

Malicious hackers are known to set up Honey Pot APs with default SSIDs (e.g. Linksys, Netgear, default, any etc), hotspot SSIDs, and even corporate SSIDs outside of buildings and watch a large number of clients automatically connect to the AP. These APs can then inflict a variety of attacks on the client or attempt password stealing by presenting a login page to the client over the mis-associated wireless connection.

Rogue Clients

Rogue clients are those that are unauthorized to attach to an authorized corporate wireless network. This may occur through an authorized access point that has been mis-configured with encryption turned off, or through an access point that has had its encryption/authentication compromised and uses the key to connect to a properly configured authorized access point.

Denial of Service Attacks

A danger to any enterprise, denial of service attacks are a threat that can wreak havoc on a large number of users simultaneously. There are various forms of wireless denial of service attacks, but they typically involve flooding a channel or channels with deauthentication or similar packets that terminate all current and attempted client associations to access points. Denial of service attacks can be particularly destructive to voice over Wi-Fi applications, completely halting the conversation.

Preventing Wi-Fi Vulnerabilities with a Wireless Intrusion Prevention System

The benefits of wireless LANs are so compelling for healthcare – improving efficiencies, lowering costs and reducing preventable medical errors - that doing without a Wi-Fi network is not a viable alternative if the institution is to continue to advance patient care and remain competitive in its region.

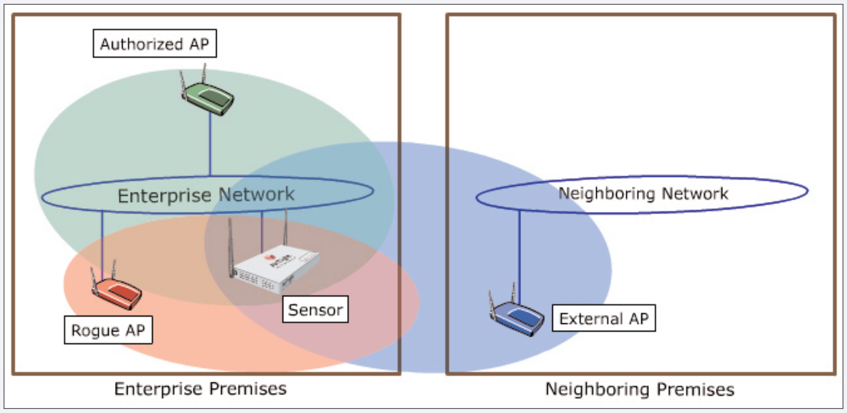
Fortunately, a new breed of security solution, the wireless intrusion prevention system (WIPS), provides a trusted 3rd party security system that prevents these Wi-Fi security risks. Much like an intrusion prevention system for wireline systems, a wireless intrusion prevention system both detects threats and automatically prevents them. WIPS solutions detect all wireless transmissions over-the-air, classify them and based on rules set up by the administrator, can automatically quarantine dangerous devices.

Wireless intrusion prevention systems stop attacks before they penetrate and harm the enterprise. WIPS solutions detect each category of attack using deterministic techniques involving a combination of device and event auto-classification, protocol analysis and association analysis. Signatures are only used to provide additional details and are not necessary for detection.

Key attributes of a wireless intrusion prevention system are:

1. **Monitoring/Detection:** All channels in the 2.4 GHz (802.11b, 802.11b/g) and 5 GHz (802.11a) bands should be scanned. It needs to analyze, aggregate, and correlate information reported by different sensors.

2. **Auto-Classification:** With increasing penetration of WLANs, there is a need to accurately and automatically sort harmful activity from the harmless activity in the shared wireless medium. As an example, in organizations with official WLAN infrastructure, the intrusion prevention system must be able to differentiate between authorized, rogue, and external wireless activities. This type of classification minimizes annoying false alarms and volumes of irrelevant alerts from the security standpoint, both of which make the security system unusable.



A Wi-Fi Intrusion Prevention System should automatically and precisely classify access points as Authorized, External and Rogue to eliminate false alerts.

3. **Prevention:** The WIPS must automatically and instantaneously block harmful wireless activity detected by its wireless sensors. For example, it must block any client from connecting to a Rogue AP or a MAC spoofing AP, prohibit formation of ad-hoc networks, and mitigate any type of DOS attack. Furthermore, it must block multiple simultaneous wireless threats while continuing to scan for new threats.

Prevention of Wi-Fi threats must be carried out with surgical precision to avoid disturbing legitimate WLAN activities. A well implemented WIPS Firewall should not stop traffic on the authorized wireless network or a neighboring Wi-Fi network.

4. **Visualization:** The spatial layout as well as materials within the enterprise (walls, columns, windows, furniture, etc.) interact with the radio coverage of the security sensor in a complex way creating a significant gap between rule-of-thumb placement and reality. A systematic, scientific, and scalable RF planning process is therefore required for determining the right placement of access points and wireless sensors. This must be site-specific and not require time consuming manual surveys. Live RF maps should provide real time information on coverage of both authorized Wi-Fi access points and security sensors.

5. **Location:** Physical remediation is a final step in permanently preventing the Wi-Fi threat and requires knowledge of the physical location of these devices. The WIPS Firewall must provide the location co-ordinates of such a device inside and around the perimeter of the enterprise premises without need for any specialized client side software or hardware.

6. **Reporting:** Detailed reporting for HIPAA compliance is a must in any WIPS system. Generated reports can help the organization prove that it has taken all steps necessary to prevent unauthorized access to patient data transmitted over networks.

How a WIPS Solution Helps Maintain HIPAA Compliance for the Wireless Network

As stated earlier, the HIPAA guidelines for network transmission require that controls be put in place for encryption, authentication, audit trail and event reporting. A WIPS solution can help ensure maintenance of HIPAA regulation 164.312 for the wireless LAN network in the following ways.

Access Controls

The Access Controls section of the HIPAA guidelines requires unique user identification and emergency access procedures. Optional requirements include automatic log off and encryption. The WIPS system can monitor and enforce the requirement for unique user identification and encryption. By using WPA or WPA2 security on the wireless LAN network, you ensure that a user-based authentication process is enforced before access to network resources is allowed. WPA or WPA2 also provide very secure TKIP or AES encryption. A WIPS solution can ensure that proper Access Control protocols stay in place by:

- Reporting and quarantining any mis-configured access points; i.e. those access points that are authorized but no longer support WPA or WPA2 security.
- Reporting and quarantining any rogue access points. Any access point that attaches to the network is not authorized should be quarantined, whether or not it has encryption enabled.
- Reporting and quarantining any client mis-associations; i.e. preventing authorized Wi-Fi clients from accidentally connecting to neighboring networks.   As an example, this will prevent a doctor's laptop from connecting to the neighboring office park Wi-Fi network that may use a standard SSID, that the doctor has also used at home or in a public hot spot.
- Reporting and quarantining any honey pot or Evil Twin access points. Malicious hackers might try to emulate authorized access points in an attempt to gain user credentials to log into the corporate WLAN network. The WIPS system should identify these types of attacks and stop any authorized client from associating with these devices.

Audit Controls

HIPAA guidelines require that systems be put in place for activity regarding protected electronic health records. Again, WPA or WPA2 security on the Wi-Fi network can be a strong foundation for ensuring that audit controls are in place. WPA and WPA2 both use IEEE 802.1x authentication which requires a RADIUS server. The RADIUS server can maintain accounting logs for all users recording the time and date that they log in and out of the network. A WIPS system can ensure enforcement of this through:

- Reporting and quarantining any mis-configured access points; i.e. those access points that are authorized but no longer support WPA or WPA2 security. This will prevent any user from gaining access to the network without being logged by a RADIUS server that can track who specifically is logging in.
- Reporting and quarantining any rogue access points. This will prevent any user from gaining access to the network without being logged by a RADIUS server that can track who specifically is logging in.
- Reporting and quarantining any ad hoc connections; i.e. preventing authorized Wi-Fi clients from connecting to other non-authorized users. As an example, if a nurse docks a Wi-Fi enabled laptop at her desk, and a client outside the hospital connects to her laptop, the person may now have access to protected electronic health records.
- Reporting and quarantining any honey pot or Evil Twin access points. Malicious hackers might try to emulate authorized access points in an attempt to gain user credentials to log into the corporate WLAN network. The WIPS system should identify these types of attacks and stop any authorized client from associating with these devices. This is especially important as once the malicious hacker has gained the user's credentials, he will look like an authorized user logging into the network.

Integrity

HIPAA guidelines suggest optional requirements to ensure that electronic medical records have not been improperly modified. As a baseline, WPA or WPA2 encryption can be enforced on the wireless LAN to ensure that data is not modified over-the-air. The WIPS solution can:

- Reporting and quarantining any mis-configured access points; i.e. those access points that are authorized but no longer support WPA or WPA2 security. This will prevent any user from gaining access to the network without being logged by a RADIUS server that can track who specifically is logging in.
- Reporting and quarantining any rogue access points. This will prevent users transmitting electronic medical records over an access point with no or weak WEP encryption.
- Reporting and quarantining any ad hoc connections; i.e. preventing authorized Wi-Fi clients from connecting to other non-authorized users. As an example, if a nurse docks a Wi-Fi enabled laptop at her desk, and a client outside the hospital connects to her laptop, the person may now have access to protected electronic health records.
- Reporting and quarantining any honey pot or Evil Twin access points. Malicious hackers might try to emulate authorized access points in an attempt to gain user credentials to log into the corporate WLAN network. The WIPS system should identify these types of attacks and stop any authorized client from associating with these devices. This is especially important as once the malicious hacker has gained the user's credentials, he will look like an authorized user logging into the network.

Person or Entity Authentication

HIPAA guidelines require that the person or entity logging into the network be authenticated. WPA and WPA2 using IEEE 802.1x require mutual authentication between the client and the network, fulfilling the baseline of this requirement. The WIPS system can enforce this policy through:

- Reporting and quarantining any mis-configured access points; i.e. those access points that are authorized but no longer support WPA or WPA2 security. This will prevent any user from gaining access to the network without being authenticated by the RADIUS server.
- Reporting and quarantining any rogue access points. Any access point that attaches to the network and is not authorized should be quarantined, whether or not it has encryption enabled.
- Reporting and quarantining any client mis-associations; i.e. preventing authorized Wi-Fi clients from accidentally connecting to neighboring networks. As an example, this will prevent a doctor's laptop from connecting to the neighboring office park Wi-Fi network that may use a standard SSID, that the doctor has also used at home or in a public hot spot.
- Reporting and quarantining any honey pot or Evil Twin access points. Malicious hackers might try to emulate authorized access points in an attempt to gain user credentials to log

into the corporate WLAN network. The WIPS system should identify these types of attacks and stop any authorized client from associating with these devices.

Transmission Security

HIPAA guidelines suggest optional requirements to ensure the integrity controls and encryption be used for the transmission of electronic health medical records. WPA with TKIP encryption and WPA2 with AES both provide for strong encryption with Message Integrity Check to ensure that the data has not been tampered with. The WIPS system can ensure that this security method remains in force through:

- Reporting and quarantining any mis-configured access points; i.e. those access points that are authorized but no longer support WPA or WPA2 security. This will prevent data tampering over systems that have no encryption or weak WEP encryption.
- Reporting and quarantining any rogue access points. This will prevent users transmitting electronic medical records over an access point with no or weak WEP encryption.

Automatically Maintaining Security Procedures and Incident Reporting

Beyond securing the wireless LAN itself, maintaining proper procedures and incident management reporting is also required by HIPAA. With the threat of rogue access points and clients accidentally associating to neighboring networks, simply monitoring the possible threats to the enterprise could be a daunting task. With a wireless IPS system, however, the burden of compliance in this area can be easily managed.

Risk Analysis and Management

HIPAA guideline 164.308(a)(1) requires that an analysis be done of the potential risks to the confidentiality and integrity of protected health information. And that measures be put in place to mitigate these risks. A wireless IPS solution provides 24 x 7 monitoring and notification of potential vulnerabilities to the corporate network from Wi-Fi threats. This constant updating ensures that not just spot checks are completed, but a true ongoing analysis of the risks is maintained. In addition, proper intrusion prevention policies can automatically mitigate all Wi-Fi threats.

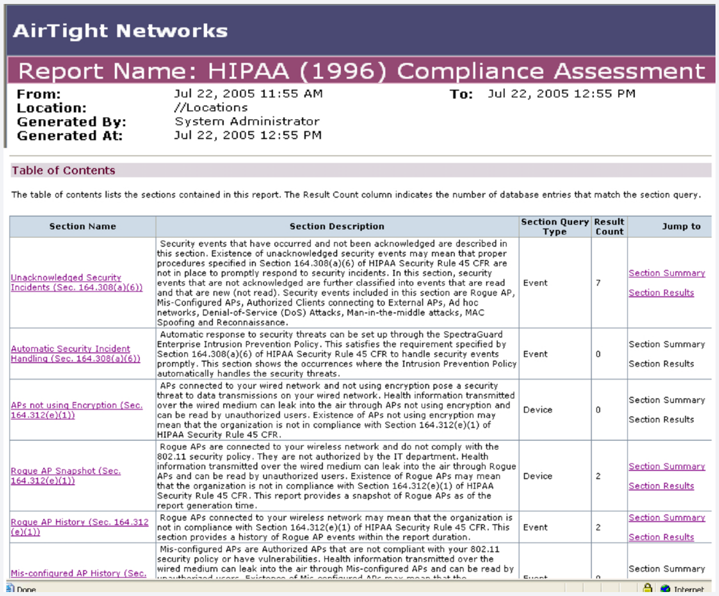
Security Incident Reporting

In section 164.308(a)(6), HIPAA requires that any security incidents be reported and that any actions taken be documented. The Wi-FI IPS system can provide:

- Reports of all security incidents, i.e. rogue access points, client mis-associations, MAC spoofing APs, etc including location, date, time and participating devices that are not addressed, and
- Reports of all security incidents that are automatically handled, again including location, date, time and participating devices

An Example Compliance Report

As discussed above, a properly configured wireless IPS system can not only provide constant monitoring, but also automatic prevention of the many threats that Wi-Fi poses to the confidentiality and integrity of healthcare records. Compliance reports tailored for all levels of management can be automatically generated. A high level view, as shown in the report below from AirTight Network's SpectraGuard Enterprise, can provide an immediate understanding of the areas that the organization faced risks.



AirTight Networks

Report Name: HIPAA (1996) Compliance Assessment

From: Jul 22, 2005 11:55 AM **To:** Jul 22, 2005 12:55 PM
Location: //Locations
Generated By: System Administrator
Generated At: Jul 22, 2005 12:55 PM

Table of Contents

The table of contents lists the sections contained in this report. The Result Count column indicates the number of database entries that match the section query.

Section Name	Section Description	Section Query Type	Result Count	Jump to
Unacknowledged Security Incidents (Sec. 164.308(a)(6))	Security events that have occurred and not been acknowledged are described in this section. Existence of unacknowledged security events may mean that proper procedures specified in Section 164.308(a)(6) of HIPAA Security Rule 45 CFR are not in place to promptly respond to security incidents. In this section, security events that are not acknowledged are further classified into events that are read and that are new (not read). Security events included in this section are Rogue AP, Mis-Configured APs, Authorized Clients connecting to External APs, Ad hoc networks, Denial-of-Service (DoS) Attacks, Man-in-the-middle attacks, MAC Spoofing and Reconnaissance.	Event	7	Section Summary Section Results
Automatic Security Incident Handling (Sec. 164.308(a)(6))	Automatic response to security threats can be set up through the SpectraGuard Enterprise Intrusion Prevention Policy. This satisfies the requirement specified by Section 164.308(a)(6) of HIPAA Security Rule 45 CFR to handle security events promptly. This section shows the occurrences where the Intrusion Prevention Policy automatically handles the security threats.	Event	0	Section Summary Section Results
APs not using Encryption (Sec. 164.312(e)(1))	APs connected to your wired network and not using encryption pose a security threat to data transmissions on your wired network. Health information transmitted over the wired medium can leak into the air through APs not using encryption and can be read by unauthorized users. Existence of APs not using encryption may mean that the organization is not in compliance with Section 164.312(e)(1) of HIPAA Security Rule 45 CFR.	Device	0	Section Summary Section Results
Rogue AP Snapshot (Sec. 164.312(e)(1))	Rogue APs are connected to your wireless network and do not comply with the 802.11 security policy. They are not authorized by the IT department. Health information transmitted over the wired medium can leak into the air through Rogue APs and can be read by unauthorized users. Existence of Rogue APs may mean that the organization is not in compliance with Section 164.312(e)(1) of HIPAA Security Rule 45 CFR. This report provides a snapshot of Rogue APs as of the report generation time.	Device	2	Section Summary Section Results
Rogue AP History (Sec. 164.312 (e)(1))	Rogue APs connected to your wireless network may mean that the organization is not in compliance with Section 164.312(e)(1) of HIPAA Security Rule 45 CFR. This section provides a history of Rogue AP events within the report duration.	Event	2	Section Summary Section Results
Mis-configured AP History (Sec.	Mis-configured APs are Authorized APs that are not compliant with your 802.11 security policy or have vulnerabilities. Health information transmitted over the wired medium can leak into the air through Mis-configured APs and can be read by unauthorized users. Existence of Mis-configured APs may mean that the	Event	0	Section Summary

Detail on each area can be provided by simply clicking on the appropriate section. This enables understanding of the exact nature of the security incidents, their location, dates, time and devices involved.

Conclusion

Healthcare is one of the most appropriate environments for wireless LANs with its naturally mobile population of doctors, nurses and other caregivers. Wi-Fi networks can bring about great benefits to staff and patients, and help healthcare institutions meet goals of reducing preventable medical errors and streamlining patient care and billing. Due to strict HIPAA requirements, care must be taken to properly secure the wireless LAN network. Beyond using the built-in measures provided by the wireless LAN system vendor, healthcare institutions should consider a third party security monitoring system to prevent common and malicious vulnerabilities. Wireless intrusion prevention systems can monitor the entire corporate air space, ensuring that only authorized devices and authorized Wi-Fi connections are made, guaranteeing security and helping to enforce HIPAA requirements.