HIPAA Compliance and Wireless Networks

White Paper
Introduction

Enterprises and users are adopting wireless local area networks (LANs) for the convenience of rapid connections without relying on wired infrastructures. With a wireless LAN, users are free to work and communicate from any location supported by a wireless infrastructure, which translates into higher worker productivity. According to one wireless LAN benefits study, wireless LAN access enables mobile workers to be connected, on average, 1.75 hours more per day. It is no surprise, then, that wireless LAN adoption is growing in the healthcare industry, where healthcare professionals must access patient records and other critical data at the point of patient care.

Yet, while wireless LANs are convenient and provide immediate connectivity for users, they also introduce unique privacy and security challenges to IT professionals. These are particularly relevant in light of the recent passage of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA is a comprehensive regulation that requires healthcare organizations to address the privacy and security concerns of electronically-stored and transmitted data.

This paper is designed to provide healthcare organizations with a guide for achieving HIPAA compliance in conjunction with their wireless LAN deployments, and answers the following questions:

- How did HIPAA come about?
- Who is covered under HIPAA?
- How is HIPAA compliance enforced?
- What specific HIPAA standards ensure the privacy and security of electronic health information?
- What are specific privacy and security threats and vulnerabilities related to wireless LAN deployments?

About HIPAA

HIPAA was originally enacted in an effort to help workers maintain continuity of health insurance coverage as they change jobs. To simplify this process, a major portion of this Act encourages the use of electronic transactions for healthcare-related information through the standardization of diagnosis and transaction codes. Another important aspect of the drive to create this standard is the need for portability and security of patient information. To address the privacy and security concerns introduced by this standardization, HIPAA includes provisions to protect patient privacy and to standardize the security of data stored electronically and transmitted via wired and wireless networks. This is a critical issue that poses major technical challenges to healthcare organizations.
HIPAA Covered Entities

Any healthcare organization that stores information electronically or uses electronic transactions is considered a covered entity and must achieve HIPAA compliance. This includes the following organizations:

- **Healthcare Providers** - hospitals, physicians, dentists, pharmacists, managed care providers, etc.
- **Healthcare Payers** - health insurance companies, managed care providers, prescription benefit management firms, etc.
- **Healthcare Clearinghouses** - organizations that act as an intermediary to translate nonstandard claims information between payers and providers

How is HIPAA Compliance Enforced?

The HIPAA standards and proposed rules outline both civil and criminal punishments, depending on intent. The Centers for Medicare and Medicaid Services (CMS) are responsible for civil punishment of HIPAA violations, while the Department of Justice is responsible for criminal punishment. HIPAA compliance can be expected to be an ongoing portion of accreditation audits.

The HIPAA security regulations were finalized and published in the Federal Register on February 20, 2003. Organizations will need to comply with these rules by February 20, 2005, with small providers having until February 20, 2006 to achieve compliance.

HIPAA Standards for the Security of Electronic Protected Health Information

The final rule outlines the following security requirements of HIPAA:

1. **Administrative Safeguards (§164.308)**
   This category covers documented, formal practices that govern the selection and execution of security measures and the conduct of personnel. This section introduces the concept of a “Chain of Trust”, which specifies that organizations that communicate with one another must have similar levels of data security.

2. **Physical Safeguards (§164.310)**
   This category focuses on the protection of physical computer systems and buildings from fire, natural disasters, and other hazards. It also covers physical access control functions, such as locks and sign-in procedures.

---

1 [http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-9497.pdf](http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-9497.pdf)
2 Smaller covered entities are defined as those with fewer than 50 employees.
3. Technical Safeguards (§164.312)
This category is especially relevant to wireless devices, networks, and applications. The processes put in place to protect data, as well as to control and monitor information access should comply with these rules. The proposed five safeguards are as follows:

A. Access Controls
This safeguard pertains to technical policies and procedures for information systems that maintain electronic protected health information. Technical policies and procedures should allow access only to those persons or software programs that have been granted access rights.

Implementation Specifications for Access Controls

Unique User Identification (Required) - Each user should be assigned a unique name and/or number for identifying and tracking identity.

Emergency Access Procedure (Required) - Organizations should establish (and implement as needed) procedures for obtaining necessary electronic protected health information (PHI) during an emergency.

Automatic Logoff (Addressable) - Organizations should implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Encryption and Decryption (Addressable) - Organizations should implement a mechanism to encrypt and decrypt electronic PHI.

B. Audit Controls
This safeguard outlines requirements to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

C. Integrity
This safeguard focuses on policies and procedures that protect electronic PHI from improper alteration or destruction.

Implementation Specifications to Ensure Integrity

Mechanism to Authenticate Electronic PHI (Addressable) - Electronic mechanisms must be implemented to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.

D. Person or Entity Authentication
Procedures must be implemented to verify that a person or entity seeking access to electronic PHI is the one claimed.
HIPAA Compliance and Wireless Networks

E. Transmission Security
This safeguard outlines technical security measures necessary to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network.

Implementation Specifications for Transmission Security:

Integrity Controls (Addressable) - Organizations should implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of.

Encryption (Addressable) - Organizations should implement a mechanism to encrypt electronic PHI whenever deemed appropriate.

Privacy and Security: Threats and Vulnerabilities

The primary security and privacy vulnerabilities of wireless LANs are summarized in the following three categories.

Mobile Content
A commonly known threat through which data can be destroyed is by using executables such as viruses, worms, and Trojan horses. A wide variety of anti-virus products are available that detect and mitigate risk from these executables. Another mobile content-related concern is the risk of system crashes and random data loss due to device corruption. This vulnerability can be overcome by system management practices such as backing up data and implementing failover systems.

Management Links
A second major category of risk of wireless LANs is the management links, whereby (a) invaders can sniff accounts and passwords by hacking into the data transfer stream over an unprotected network; and (b) hijackers can break into these links and acquire unauthorized server control. Though these risks are significant, they can be mitigated through the use of data encryption.

Data Integrity, Confidentiality, and Authenticity
In a typical wireless LAN implementation, data travels from mobile device to access point without being checked for integrity; it is then forwarded without being authenticated. Naturally, to allow unauthenticated data access and manipulation is to engage in faulty network configuration and change control.

Healthcare providers and other organizations face the following challenges in implementing a security solution:
Users such as doctors, care givers, and administrative staff must be insulated from technical details, so that they can focus on providing quality health care services to their patients.

Wi-Fi technology is evolving so rapidly that upgrading the security system to incorporate new standards is resource-intensive.

Due to challenging economic conditions, IT departments have access to limited resources and financial budgets.

**Achieving HIPAA Compliance for Wireless LANs**

Technical Safeguards (§164.312) is the most relevant category of the HIPAA Standards for the Security of Electronic Protected Health Information. This section illustrates the best practices that enable organizations to comply with these strict standards. A properly configured security solution will enable an organization to achieve compliance. It will also mitigate emerging risks due to vulnerabilities in wireless security.

The following table lists the Technical Safeguards and the specific implementation specification for each safeguard. Varieties of technical solutions exist, which alone or in combination can satisfy each of the technical specifications. The last column in the table below exemplifies the best practices to accomplish each of the implementation specifications based on the following criteria:

1. Provides robust protection against the threats and vulnerabilities as discussed in “Privacy and Security: Threats and Vulnerabilities” section. Layer 2 Encryption makes the wireless network unbreakable by creating a virtual and impenetrable wall for every connection.

2. Leverages existing investment in authentication databases such as directory servers and RADIUS servers. Commonly used directory servers include Microsoft Active Directory, Microsoft NT Domain Server or any LDAP compliant directory. RADIUS-compliant servers include Cisco Secure ACS, Funk Steel Belted RADIUS, Interlink Secure XS, Microsoft Internet Authentication Services, etc.

3. Supports an open, non-proprietary architecture that is compatible with any mix of 802.11a, b, g, h, or j access points. It should also work with access points from any manufacturer. This approach protects customers’ existing infrastructure investments, resulting in overall reduced cost of ownership.

4. Accommodates the wide range of network management needs such as multiple access levels, multiple user groups, monitoring and control.

5. Provides a simple user interface for the end user as well as network managers.
<table>
<thead>
<tr>
<th>Technical Safeguard</th>
<th>Implementation Specification</th>
<th>Best Practices For Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Access controls</td>
<td>Emergency access procedure</td>
<td>Distributed Architecture</td>
</tr>
<tr>
<td>A. Access controls</td>
<td>Automatic logoff</td>
<td>Configurable Idle Timeout</td>
</tr>
<tr>
<td>A. Access controls</td>
<td>Unique user identification</td>
<td>Authentication services</td>
</tr>
<tr>
<td>A. Access controls</td>
<td>Encryption and decryption</td>
<td>Advanced Encryption Standard(AES)</td>
</tr>
<tr>
<td>B. Integrity</td>
<td>Mechanism to authenticate electronic PHI</td>
<td>Layer 2 Encryption</td>
</tr>
<tr>
<td>B. Integrity</td>
<td>Integrity controls</td>
<td>Advanced Encryption Standard(AES)</td>
</tr>
<tr>
<td>C. Audit Controls</td>
<td>Record and examine activity</td>
<td>Real-time Monitoring</td>
</tr>
<tr>
<td>D. Person or Entity Authentication</td>
<td>Unique user identification</td>
<td>Directory Integration</td>
</tr>
<tr>
<td>E. Transmission Security</td>
<td>Encryption and decryption</td>
<td>Layer 2 Encryption</td>
</tr>
<tr>
<td>E. Transmission Security</td>
<td>Integrity controls</td>
<td>Advanced Encryption Standard(AES)</td>
</tr>
</tbody>
</table>

**Best Practices in Implementing Technical Safeguards (§164.312)**

The lifecycle of a typical wireless LAN security implementation consists of three phases:

a. Installation and set up of the security solution
b. Secured data communication over the wireless LAN
c. Monitoring and control by the network administrator

These phases are illustrated in the diagram below:

**Phase 1: Installation and Set up**

In this phase, the security solution is installed and integrated with other software systems, such as RADIUS servers, Windows NT Domain, Microsoft Active Directory, or other...
LDAP-compliant directory servers. The policies for various groups should be set based on role. Following are the best practices that should be adopted in light of HIPAA regulations such as access control (§164.312a), person or entity authentication (§164.312d), and transmission security (§164.312e).

**Configurable Idle Timeout**
Administrators should be able to configure very short idle timeout values to ensure that a user who leaves the mobile device idle is not placing the device (or network resources) at undue risk. For instance, a healthcare worker who leaves an authorized tablet PC connected during a lunch break may be placing the hospital at risk of violating HIPAA security regulations.

**Directory Integration**
Network administrators should leverage user credential and role information already available in existing enterprise directories. Additional databases of user or device information should not be required to provide highly-granular, role-based access control.

**Distributed Architecture**
Implementing a distributed architecture will optimize system behavior in the event of a component failure. For example, integration with a RADIUS server is not required for ongoing session connectivity, so a failure of RADIUS server connectivity affects only the creation of new sessions. The existing sessions are unaffected and will remain operational until they expire.

**Failover**
For high-availability, organizations should deploy redundant servers to act as backups for the primary security server. In the event of a hardware failure, the backup server should activate automatically, without disrupting existing users.

**Role-Based Firewall**
To provide flexible, role-based authorization control, administrators should apply a unique firewall to each wireless access policy. Using this role-based firewall to restrict access based on server, subnet, application, or TCP/UDP/ICMP port, administrators should control session traffic in a highly-granular fashion regardless of user location.

**Phase 2: Secured Wireless Communication**
This phase is characterized by ongoing day-to-day activities performed by the mobile user that involves transmission of data over a wireless LAN. All transmitted data should be encrypted and authenticated, and user sessions should be maintained even as users roam across subnets. The relevant HIPAA regulations during this phase of the wireless LAN lifecycle include access control (§164.312a), integrity (§164.312b), person or entity authentication (§164.312d) and transmission security (§164.312e).
Advanced Encryption Standard (AES)
Where possible, the Advanced Encryption Standard (AES) should be used to protect sessions and networks from attack and compromise. AES is ideal for lightweight hardware devices such as PDAs, ensuring maximum battery life and throughput. Due to its performance characteristics, AES is being specified as the data privacy algorithm in the forthcoming 802.11i security standard.

Authentication Services
User identities should be verified within an Extensible Authentication Protocol - Tunneled Transport Layer Security (EAP-TTLS) tunnel to protect against capture of authentication credentials during transmission and to prevent hijack by attackers. Once a connection has been established, each frame should be authenticated to protect the integrity of the session.

Layer 2 Encryption
Full Ethernet frames, rather than just IP payloads, should be encrypted at Layer 2. This hides vital information such as IP addresses, applications, and ports from unauthorized listeners. Frame-level encryption also protects non-data network traffic, including DHCP requests or ARP messages, from being compromised and used to attack the network. Unlike IPSec-based solutions, frame-level encryption allows the easy native use of other protocols, such as IPX, AppleTalk, etc.

Unique Session Keys
Two unique key pairs should protect every active session. One key pair should encrypt and authenticate each individual frame, while the other key pair should protect the actual user data. Within a key pair, one key should be used for transmitted traffic while the other should support received traffic.

Phase 3: Monitoring and Control
Network managers should be able to observe connected users and communication activities in real-time. These activities can be recorded and the data should be stored periodically on storage devices. The Audit Control (§164.312.c) Technical Safeguard under HIPAA is dedicated to monitoring and control.

Real-Time Monitoring
A centralized management interface should make all system monitor and management functions securely available to network administrators. Administrators should be forced to authenticate in order to access this system. Once authenticated, they should be able to monitor real-time system performance and usage of the secure wireless network and make real-time adjustments to optimize the network and accommodate unexpected behavior.
Logging and Alerting
Network administrators should be able to configure settings for activity logs and alerts. Activity logs should include changes in the configuration settings for access points, gateways, network users, authentication policies, etc. An example of wireless activity that should be recorded in the logs includes detailed per-user session statistics. Alerts should include the date and time, risk level, type, and the description. Alerts should be delivered in real-time via a communication media, such as e-mail or pager.

Conclusion
All large and small healthcare organizations, including healthcare providers, healthcare payers and clearinghouses must comply with the HIPAA regulations by February 20, 2006. The Technical Safeguards as described in the HIPAA regulation §164.312 should be implemented to protect the privacy and security of health data. When correctly configured, these Technical Safeguards also mitigate risks exposed by wireless LAN vulnerabilities.

The selection process of desired technical solutions should emphasize considerations such as ease of use and compatibility with existing and emerging Wi-Fi standards. They should also leverage existing IT investments in wired and wireless network infrastructure, as well as enterprise software systems. The ideal security solution incorporates all the best practices discussed in this paper.

Cranite Systems has analyzed the HIPAA requirements and security vulnerabilities of wireless LANs. The Cranite WirelessWall solution is designed to cost-effectively address all of these essential security and ease of use features.