



White Paper

# HIPAA Compliance for the Wireless LAN

**JUNE 2015**

This publication describes the implications of HIPAA (the Health Insurance Portability and Accountability Act of 1996) on a wireless LAN solution, and highlights how Meraki products can help customers maintain a HIPAA-compliant network. The target audience of this publication is healthcare IT administrators who are responsible for the design and implementation of a wireless network.

# Table of Contents

<b>1</b>	<b>Overview</b>	3
<b>2</b>	<b>Background</b>	4
<b>3</b>	<b>Technical Safeguards</b>	6
	3.1 Unique User Identification	6
	3.2 Emergency Access	6
	3.3 Automatic Logoff	6
	3.4 Authentication, Integrity, and Encryption	6
	3.5 Audit Controls	7
<b>4</b>	<b>Administrative Safeguards</b>	8
	4.1 Log-In Monitoring	8
	4.2 Password Management	8
	4.3 Response and Reporting	8
	4.4 Data Backup and Recovery	8
	4.5 Emergency Mode Operation	9
<b>5</b>	<b>Physical Safeguards</b>	10
	5.1 Facility Security Plan	10
	5.2 Media Re-use	10
<b>6</b>	<b>Providing a HIPAA-Compliant Wireless LAN with Meraki</b>	11
	6.1 Technical Safeguards	11
	6.2 Administrative Safeguards	12
	6.3 Physical Safeguards	12

# 1 Overview

HIPAA (the Health Insurance Portability and Accountability Act of 1996) calls for the establishment of national standards for technology involved in health care transactions in order to protect the health information of individuals. HIPAA applies to any healthcare facility that exchanges patient health information. HIPAA's objective is to ensure that health information remains private and secure.

Achieving this objective involves not only implementing policies and procedures for personnel, workflows, and inventory, but also evaluating physical assets to ensure that every piece of equipment will play its part in enabling HIPAA compliance. A wireless LAN is no exception. Wireless hardware, such as access points (APs) that are installed around a facility, must facilitate HIPAA compliance. Similarly, wireless software must support the security and management features that the facility requires to enforce HIPAA compliance.

This whitepaper summarizes the key tenets of HIPAA that are relevant to a wireless LAN, describes the wireless features that can assist in satisfying these requirements, and shows how Meraki products can be used to help build a HIPAA-compliant wireless network.

## 2 Background

Enacted by the U.S. Congress in 1996, HIPAA comes in two parts: Title I and Title II. Title II of HIPAA strives to reduce health care fraud and abuse. Subtitle F of Title II is known as the “Administrative Simplification” provision, which requires the establishment of national standards for electronic health care transactions, along with national identifiers for various health care entities (e.g., providers, health insurance plans, etc.). Administrative Simplification defines 5 “rules”, one of which is the Security Rule, which describe the requirements related specifically to electronically protected health information.

The Security Rule identifies 3 types of security safeguards required for compliance:

1. **Administrative safeguards** define personnel and management processes to train employees who come into contact with private health information, as well as procedures for detecting and handling privacy violations.
2. **Physical safeguards** are policies and procedures that govern the addition and removal of hardware, access to equipment, etc.
3. **Technical safeguards** are guidelines for data encryption, data corroboration, and audit logging.

However, HIPAA does not provide specific, technical guidance. HIPAA defines the policy that must be implemented; the actual implementation (i.e., “codification”) of this policy is left to the Code of Federal Regulations (CFR). CFR Title 45, Part 164 is called “Security and Privacy”. Subpart C of this section, “Security Standards for the Protection of Electronic Protected Health Information”, translates HIPAA’s 3 security safeguards (administrative, physical, and technical) into actionable requirements that a wireless LAN must satisfy. Specifically, the regulation supplements each HIPAA safeguard with a list of “standards”, and each standard may consist of one or more “implementation specifications”, which are designated as either “required” or “addressable” (i.e., to be implemented if applicable).

The implementation specifications relevant to a wireless LAN are listed below and described greater detail in the following sections. (Each section begins by listing the implementation specifications addressed in parentheses.) The technical safeguards define the greatest number of implementation specifications that impact the wireless LAN, so that section is addressed first. Many of the other implementation specifications are outside the scope of a wireless LAN because they either pertain to overarching security policies and processes (e.g., workforce clearance procedure) that are not technology-specific, or they pertain to a different technology area that is not related to wireless connectivity (e.g., protection from malicious software).

APPENDIX A TO SUBPART C OF PART 164—SECURITY STANDARDS: MATRIX

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
<b>Administrative Safeguards</b>		
Security Management Process .....	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility .....	164.308(a)(2)	(R)
Workforce Security .....	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management .....	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training .....	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures .....	164.308(a)(6)	Response and Reporting (R)
Contingency Plan .....	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation .....	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement.	164.308(b)(1)	Written Contract or Other Arrangement (R)
<b>Physical Safeguards</b>		
Facility Access Controls .....	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use .....	164.310(b)	(R)
Workstation Security .....	164.310(c)	(R)
Device and Media Controls .....	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
<b>Technical Safeguards</b> (see § 164.312)		
Access Control .....	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)

## 3 Technical Safeguards

All but one of the implementation specifications for the technical safeguards should be addressed by a wireless LAN. However, because of the importance of this section, all the implementation specifications will be addressed.

### 3.1 Unique User Identification

(Access Control: Unique User Identification)

This specification requires a system that passes private health information to control access on a per-user basis. Within a wireless LAN, each user must be assigned a unique username and strong password and must use these credentials to access the wireless network. The wireless LAN should also be able to track these users in a log of user activity (e.g., successful and failed authentication attempts, association and disassociation times, etc.). Finally, the wireless LAN should be able to provide different levels of access to different groups of users. For instance, guests should obtain Internet-only connectivity from the wireless network, without any ability to reach private health information.

Employees, on the other hand, might be granted broader access to the network. A wireless LAN can provide this access control by broadcasting different SSIDs (the wireless networks that a client device detects), allowing an administrator to configure different access control settings on each SSID.

### 3.2 Emergency Access

(Access Control: Emergency Access Procedure)

An emergency access procedure allows personnel to access private health information during an emergency. A wireless LAN may assist with this requirement by providing LAN access to wireless users, even if connectivity to the public Internet is down. In this way, personnel can wirelessly access health information that may be stored on local file shares during an emergency. This “always up” capability is revisited as part of the emergency mode operation plan, which is specified as part of the administrative safeguards.

### 3.3 Automatic Logoff

(Access Control: Automatic Logoff)

Automatic logoff terminates a user’s session after a predetermined time of inactivity. This feature is most relevant to the application that provides the user with access to private health information. A wireless LAN may perform its own automatic logoff to disconnect a user after a preconfigured period of time.

### 3.4 Authentication, Integrity, and Encryption

(Access Control: Encryption and Decryption, Integrity: Mechanism to Authenticate Electronic Protected Health Information, Person or Entity Authentication, Transmission Security: Integrity Controls, Transmission Security: Encryption)

The objective of all the implementation specifications is to provide authentication to ensure that information is accessed by a trusted or approved user, integrity to ensure

that information is not altered in transit, and confidentiality to prevent a “man in the middle” from stealing information as it is transmitted. All 3 attributes are intrinsically connected; as such, they should be satisfied simultaneously and comprehensively, rather than piecemeal.

Best practices for user authentication include 802.1X (also known as WPA2-Enterprise), which uses public key infrastructure (PKI) to authenticate endpoints, provide integrity through digitally signed data packets, and negotiate cipher keys for the strongest encryption possible (i.e., 256-bit AES). Older authentication and encryption methods have some downsides. WPA2 with a pre-shared key (WPA2-PSK, also called WPA2-Personal) provides sufficient encryption with a suitably long and complex key, but pre-shared keys can easily be shared with other (potentially unauthorized) users. A less problematic variation is to use WPA2-PSK with a splash page that requires a user to enter username/password credentials. It is highly recommended that WEP not be used in an organization concerned about HIPAA. Not only does WEP suffer from the same ease of key sharing among users as WPA2-PSK, but with today’s processor speeds, it is also far too easy to crack a WEP key. The bottom line: Use (1) 802.1x or (2) WPA2-PSK with username/password splash page login.

### **3.5 Audit Controls**

(Audit Controls)

Audit controls enable an administrator to monitor user activity on systems that access private health information. A wireless LAN should provide a log of user-level events, such as associations, authentications, and bandwidth usage. The log should be descriptive enough to allow an administrator to pursue the appropriate remediation steps (e.g., block the device, contact the user, etc.).

## 4 Administrative Safeguards

The administrative safeguards are mostly concerned with the management procedures and processes that govern how private health information is handled. A few of the implementation specifications defined as part of administrative safeguards have implications for the wireless LAN.

### 4.1 Log-in Monitoring

(Security Awareness and Training: Log-in Monitoring)

Log-in monitoring calls for record-keeping of the administrators who access any systems that transmit or store private health information. For a wireless LAN, these records are important for forensic analysis. For instance, an administrator might inadvertently disable encryption on the wireless network, which could allow an eavesdropper to capture private health information over the air. A record of administrator logins (both successful and unsuccessful) and their configuration changes allows an organization to determine who made the configuration change to disable wireless encryption and when the change took place, which identifies the exposure time of the misconfiguration.

### 4.2 Password Management

(Security Awareness and Training: Password Management)

Password management requires procedures for creating, changing, and safeguarding administrative passwords. Every wireless LAN should be able to provide this capability in a scalable and centralized way. Rather than replicating administrative accounts on individual APs (as is the case with “autonomous” or “fat” APs), a centralized management solution should be sought, which manages and stores administrative accounts to access all APs across the entire network.

### 4.3 Response and Reporting

(Security Incident Procedures: Response and Reporting)

A mechanism is needed to alert administrators to suspected or known security incidents, to mitigate the incidents as much as possible and to document the incidents and their outcomes for future analysis. A wireless LAN should provide as much information to administrators as possible through these alerts. Security alerts should report on security incidents that pertain to administrators, (e.g., excessive administrative login attempts), wireless users (e.g., excessive user login attempts), and wireless devices (e.g., rogue AP detection). Management alerts should report on any events that are actionable by administrators—for instance, if an AP goes down.

### 3.4 Authentication, Integrity, and Encryption

(Contingency Plan: Data Backup Plan, Contingency Plan: Disaster Recovery Plan)

These implementation specifications call for procedures to back up data and recover data after the emergency is over. For a wireless LAN, the most critical data typically resides in the management interface and may consist of configuration, administrative accounts, and user accounts. (Larger organizations would likely store and manage user accounts on a dedicated authentication server, such as Active Directory. This server would have to be backed up separately.) A controller-based wireless LAN typically provides an administrator



with the ability to export a configuration file off of the controller. This configuration file can be uploaded back to the controller in order to restore settings. Alternatively, a cloud-managed wireless LAN should provide this data backup to an organization transparently through redundant systems in multiple geographically distributed data centers.

#### **4.5 Emergency Mode Operation**

(Contingency Plan: Emergency Mode Operation Plan)

Systems should be able to tolerate failures and outages gracefully during emergencies. Systems should remain operational as much as possible so that private health information can still be accessed. The need for a wireless LAN to continue operating when the public Internet is unavailable was discussed as part of technical safeguards. Here, the architectural and administrative implications of providing an “always up” wireless LAN are considered. At a high level, a wireless LAN should eliminate single points of failure. A common limitation of controller-based wireless LANs is that the controller must be reachable by the APs in order for the wireless network to remain operational. As such, administrators often find themselves deploying redundant standby controllers that take over when the primary controllers go down—a deployment with significant cost and management implications. More preferable is an architecture that eliminates the controller as a single point of failure. In general, a cloud-managed wireless LAN allows the APs to remain operational (i.e., providing wireless access to users), even when connectivity to the cloud-based management interface is unavailable.

## 5 Physical Safeguards

The implementation specifications for physical safeguards are generally outside the scope of the wireless LAN. They relate mostly to controlling access to facilities and equipment—in particular, those that store private health information. However, the implementation specifications below should be addressed by a wireless LAN.

### 5.1 Facility Security Plan

(Facility Access Controls: Facility Security Plan)

The facility security plan describes the need to secure physical property and equipment from unauthorized physical access, tampering, and theft. In a wireless LAN, the APs are the components that are generally most prone to tampering. APs should be secured by locks (e.g., Kensington locks and mounting brackets) and positioned out of reach of users. Example mounting locations include high on walls, on ceilings, or inside the plenum (if the APs are plenum-rated). For a controller-based wireless LAN, the controller is the most expensive piece of hardware in the network. As such, it also needs to be secured, typically inside an access-restricted data center. Besides being a target for theft and tampering, the controller is also a target for network security breaches. Many security vulnerabilities have been identified with wireless LAN controllers over the years. Gaining access to a controller can compromise not just the wireless LAN, but even the entire network. Organizations that want to minimize their security exposure should consider a cloud-managed wireless LAN, which eliminates the need for a controller altogether.

### 5.2 Media Re-use

(Device and Media Controls: Media Re-use)

If a system stores private health information, there needs to be a way to clear that information before the system is reused for a different purpose. For a wireless LAN, the implication is simple: ideally, no component of the wireless LAN should ever store user data.

## 6 Using Meraki in Your HIPAA-Compliant Wireless LAN

Meraki's cloud-managed APs enable an organization maintain a wireless LAN that can satisfy HIPAA's implementation specifications. The requirements described earlier are revisited below to show how Meraki can be used in your network.

### 6.1 Technical Safeguards

REQUIREMENT	HOW MERAKI FITS IN
Unique User Identification	Meraki APs can broadcast up to 15 SSIDs simultaneously, each with its own security, network, and access control settings. In addition, individual network group policies, VLAN assignment, and MDM integration provide granular security control. For authentication, Meraki supports 802.1x and username/password login via a splash page. User credentials can be validated against either a customer-premise authentication server (such as Active Directory, LDAP, or RADIUS) or a Meraki-hosted authentication server. Through the Meraki Cloud, an administrator can obtain a log of the users and devices that have connected to the Meraki wireless network, and view a history of network usage.
Emergency Access	The Meraki wireless LAN stays up, even if connectivity to the Meraki Cloud becomes unavailable. Users can continue accessing LAN resources without interruption.
Authentication, Integrity, and Encryption	Meraki supports WPA/WPA2-Enterprise (802.1x) with strong 256-bit AES encryption and WPA/WPA2-Personal (pre-shared key). Communication between the APs and the Meraki Cloud is conducted over a secure SSL connection.
Audit Controls	A customer network administrator can see events related to wireless users on the Meraki network, including wireless associations/disassociations, authentication attempts, DHCP requests/renewals, and traffic initiation.

## 6.2 Administrative Safeguards

REQUIREMENT	HOW MERAKI FITS IN
Log-in Monitoring	The Meraki Cloud provides a log of administrative activity, including logins and configuration changes. In addition, different privilege levels (read-only and full read-write access) can be specified for different administrators. Granular administrative privileges can be flexibly applied by network tag.
Password Management	A customer network administrator can create, modify, and delete other administrator accounts through the Meraki Cloud. A single account can be used to configure and monitor thousands of Meraki APs in a single network. The Meraki Cloud can also be configured to enforce password complexity requirements, account lockout thresholds, password expiry, and two-factor authentication.
Response and Reporting	A whole suite of security and management alerts can be communicated to administrators, including rogue AP detection and AP outages. Live tools enable an administrator to troubleshoot an AP in a remote office without requiring any on-site resources.
Data Backup and Recovery	The Meraki Cloud is hosted in multiple geographically distributed data centers for high availability and reliability.
Emergency Mode Operation	A wireless LAN built using Meraki APs does not require any hardware-based wireless LAN controllers, reducing physical and network security risk.

## 6.3 Physical Safeguards

REQUIREMENT	HOW MERAKI FITS IN
Facility Security Plan	Each Meraki AP comes with a security screw, Kensington lock hard point, and a padlock hard point. Models are available with Plenum rating.
Media Re-use	No user traffic is ever stored on a Meraki AP, nor does user traffic flow back to the Meraki Cloud.

For more information on how Meraki can help you build a HIPAA-compliant wireless network with Meraki APs, please contact an authorized Meraki partner. Or, you can contact Meraki directly at 1.888.490.0918 or [www.meraki.cisco.com](http://www.meraki.cisco.com).