Aerohive NETWORKS

# Wireless LAN Best Practices for Compliant Care

## Cooperative Control and the Rx for HIPAA

## Introduction

Innovations in healthcare have greatly improved patient care and increased the rate of survival for patients who may have previously been left without hope. These advances range from new medical procedures to cutting-edge technology such as digital imaging equipment available bedside, and all of them strive to decrease frustrating wait times and mistakes while increasing clinicians' abilities to save lives.

Wireless LANs, when coupled with Electronic Medical Records, Location Asset Tracking, Voice, and other technologies, play a key role in healthcare innovation because they provide the ability to access information from a variety of sources regardless of user privilege, help decrease costly and sometimes impractical wired infrastructure throughout the campus, and increase efficiency.

WLANs are no longer an optional convenience for a hospital network, but rather a critical part of the network infrastructure that administrators, clinicians, patients, and many others depend upon to provide state-of-the-art medical care.

## Why Wi-Fi in Healthcare?

Across the globe, the drivers for implementing technology in healthcare are generally the same: improve patient care, adhere to regulatory compliance requirements, and the ever-present goal of decreasing costs.

The United Kingdom (UK) was one of the first countries to require Electronic Medical Records across all the national health facilities with the Electronic Records Development and Implementation Programme in 2003. The purpose of the requirement was to ensure patient records were available to clinicians across the country whenever the patient sought or required care. Despite the noble goal, the program has come under a lot of scrutiny because of the potential patient privacy concerns, and has led both the EU and other countries, including the USA, to focus on patient privacy as a major factor when implementing technology in healthcare facilities.

The American Recovery and Reinvestment Act (ARRA) of 2009 included a key component specifically targeted at healthcare IT, which is known as the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act covers a broad range of healthcare IT initiatives including providing over $20 billion in funding towards implementation of healthcare IT. HITECH was created in addition to the existing Health Insurance Portability and Accountability Act (HIPAA) requirements for data security, and instituted several levels of fines if not completely implemented by facilities by 2015.

The goal of both HIPAA and HITECH is to secure Protected Health Information (PHI) and electronic protected health information (ePHI) while it traverses the various networking, security, and other devices both within a healthcare facility network and between healthcare providers/facilities. While HIPAA and HITECH only pertain to the USA, the security of healthcare information is certainly an international concern and many of the compliance requirements translate across country and language borders to ensure completely reliable, secure, and fast access to information and resources that can help to improve patient care and ultimately save lives.

Many of the advances in technology designed to improve patient care are also subject to the most stringent compliance requirements. Electronic Medical Records (EMR) and Bar Code Medicine Administration (BCMA) are two great examples of technological enhancements that focus on providing more immediate and accurate access to patient data, and are two of the major drivers for healthcare facilities to implement wireless LAN technology. Other major drivers include secure and reliable voice over Wireless LAN (VoWLAN), RFID Monitoring, Location Asset Tracking, and of course, wireless access for devices such as smart phones, tablets, and laptops both by patients and hospital staff.

- **Electronic Medical Records**, also known as Electronic Health Records, are one of the most critical components of a patient's success in a healthcare facility, and are subject to the most strict security

standards. These records document all healthcare aspects of a patient and need to be readily accessible while still being completely secure from unauthorized access.

- **Bar Code Medication Administration** is vital to ensuring patient safety and accuracy of prescription fulfillment, as it nearly eliminates the chance of mistaken identity or inappropriate delivery of medication to a patient.
- **Secure and reliable communication** between clinicians and healthcare employees is necessary to provide quality healthcare to patients. The proliferation of Voice over WLAN (VoWLAN) devices is mainly due to their ability to provide immediate communication without requiring deployment or maintenance of costly parallel DECT or 900Mhz access points. VoWLAN devices can enable paging and signaling between doctors, nurses, patients, and staff without having to disturb an entire ward, and also often have significantly better coverage in hospital environments than standard mobile phones.
- **Location Asset Tracking** provides hospitals with a way to identify and locate important tools such as wheelchairs, IV pumps, mobile medical equipment, and sometimes even wandering patients. Along with location, it is also possible to monitor temperature, condensation, and other types of environmental characteristics that may impact pharmacological or patient health, and which are a critical part of healthcare standards compliance.
- **BYOD Access** for personal wireless devices is also an important driver for wireless LANs in healthcare. Just like the local coffee shop, patients are more likely to choose a facility that provides them easy access to information and entertainment using their laptops and portable mobile devices than a facility that does not. It has become an expectation that wireless access will be available for patients, staff, and guests rather than simply a nice amenity.

Because of all these technologies and the many more to come require wireless networks in healthcare facilities, countries have had to designate best practices for technology usage. In Europe, the EU already has strict guidelines for data security (Health and Social care Act 2012, Directive 95/46/EC) and has extended those to apply to Healthcare. In the USA, while HIPAA defines the policy for how electronic protected health information (ePHI) should be protected, the actual "how-to" guidelines are contained in Code of Federal Regulations (CFR) Title 45. In section 164, Security and Privacy, the Security Standards for the Protection of Electronic Protected Health Information details the 3 major security safeguards from HIPAA (Administrative, Physical, and Technical) and the requirements for compliance[1].

All of these guidelines in the CFR and the data security requirements from the EU circle around some basic best practices, which include validation of networks for use with medical equipment, determining acceptable latency and load qualifications for the network, and providing detailed reporting information to prove compliance or violation of the policies.

## Best Practices for HIPAA-Compliant Networking

As mentioned above, there are three major components to complying with the US HIPAA standards: Administrative, Physical, and Technical[2].

- **Administrative safeguards** are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.
- **Physical safeguards** are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
- **Technical safeguards** include technology-related measures to protect an entity's network and devices from data breaches and unauthorized access.

1 http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=b6bd13b5b652fe09e86dd86c442eeb62&rgn=div6&view=text&node=45:1.0.1.3.79.3&idno=45
2 same as above

The administrative and physical safeguard guidelines pertain mostly to protecting the ePHI data itself and properly training the staff accessing it, but there are a few guidelines that affect the implementation of the wireless network. The majority of the applicable requirements for networking systems that contain ePHI content reside in the technical safeguards section. Listed below are the requirements and how Aerohive addresses them.

## § 164.308 Administrative safeguards[3]

**(D) Information system activity review (Required) -** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Historical and real-time reports are available in Aerohive's HiveManager NMS for configurable time periods, and can be easily exported in .csv or .pdf format or emailed directly to an administrator responsible for implementing compliance procedures.

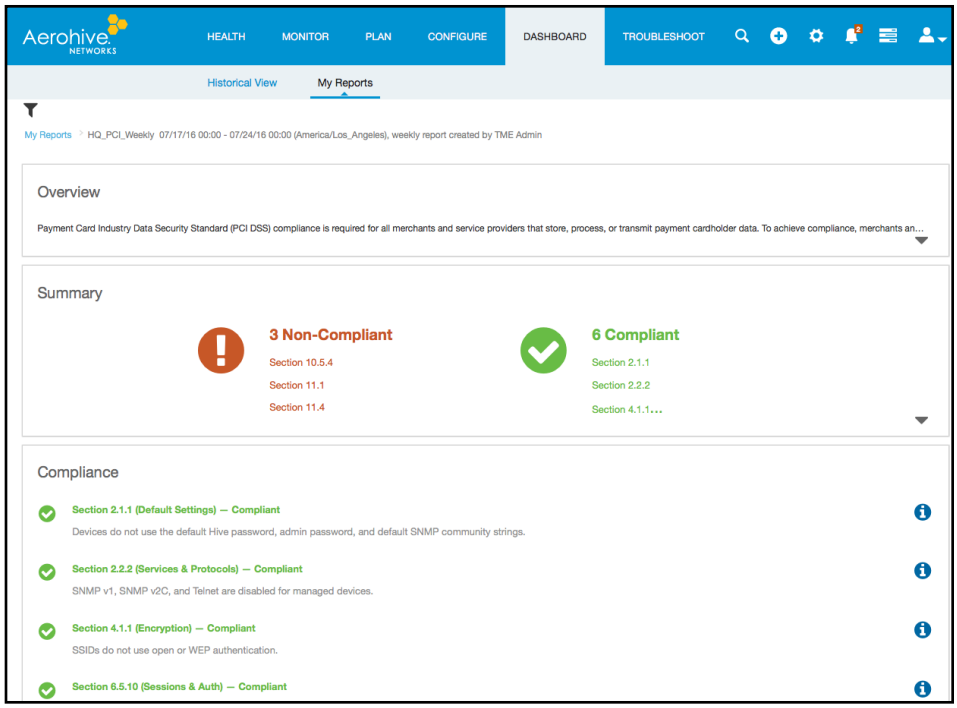
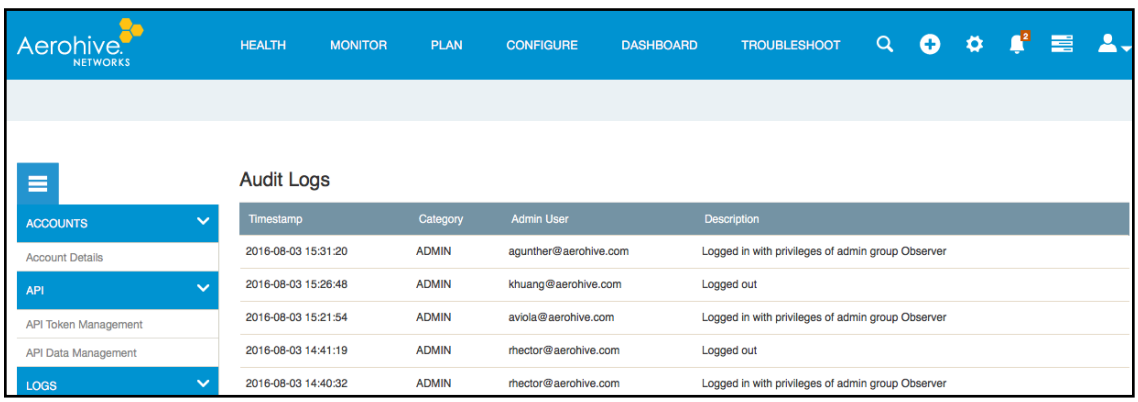



Figure 1: Compliance report

**(C) Log-in monitoring (Addressable) -** Procedures for monitoring login attempts and reporting discrepancies.

Aerohive devices can log and report on all network access attempts and track the information in client historical reports. HiveManager keeps a detailed audit log of all administrator activity, which can be sorted by timeframe, administrator, or action.




3 http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=b6bd13b5b652fe09e86dd86c442ee-b62&n=45y1.0.1.3.79&r=PART&ty=HTML#45:1.0.1.3.79.3.27.4

Figure 2: Audit Log

**(D) Password management (Addressable) -** Procedures for creating, changing, and safeguarding passwords.

Passwords stored in HiveOS and HiveManager are obscured, and both HiveOS and HiveManager support external authentication against a RADIUS server and user store, which can force scheduled password changes.

**(ii) Implementation specification: response and reporting (Required)** - Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

Real-time alerts and dashboard updates are available to administrators to track network security information as well as application usage and network access. In addition, Aerohive can automatically mitigate detected rogue access points or clients that are not authorized to be on the network, as well as provide location information for where the rogue access points or clients are located on the network to aid an administrator in a positive outcome.

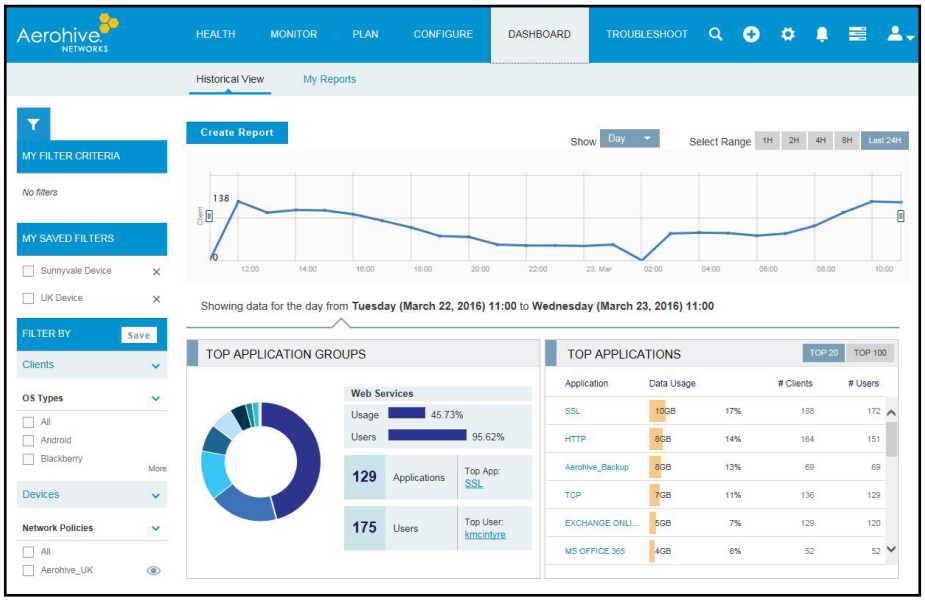



Figure 3: Dashboard view

**(C) Emergency mode operation plan (Required) -** Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

Aerohive devices are fully resilient and redundant and do not rely on any central entity that could be a single point of failure. The devices operate with or without access to the central network management system, and can even perform mission-critical functions like RADIUS and user authentication caching to ensure continued secure access to the network even in the event of an emergency condition.

## § 164.310 Physical safeguards[4]

**(ii) Facility security plans (Addressable)**. Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

All Aerohive access points are plenum rated and can be secured by Kensington-style locks. In addition, they include a tamper-proof security screw and for the devices with USB support, the USB can be covered and secured as well.

**(iii) Access control and validation procedures (Addressable).** Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

Aerohive devices enable admins to create very granular access rules based on available context, including user identity, device type, ownership, location, and time of day. Using any combination of the available context, administrators can define exactly who, what, when, and where users can connect to specific network resources by defining stateful firewall and Quality of Service (QoS) policies built right into HiveOS. In addition, these policies can implement VLAN or network assignment, tunneling permissions, and even SLAs based on the available context.

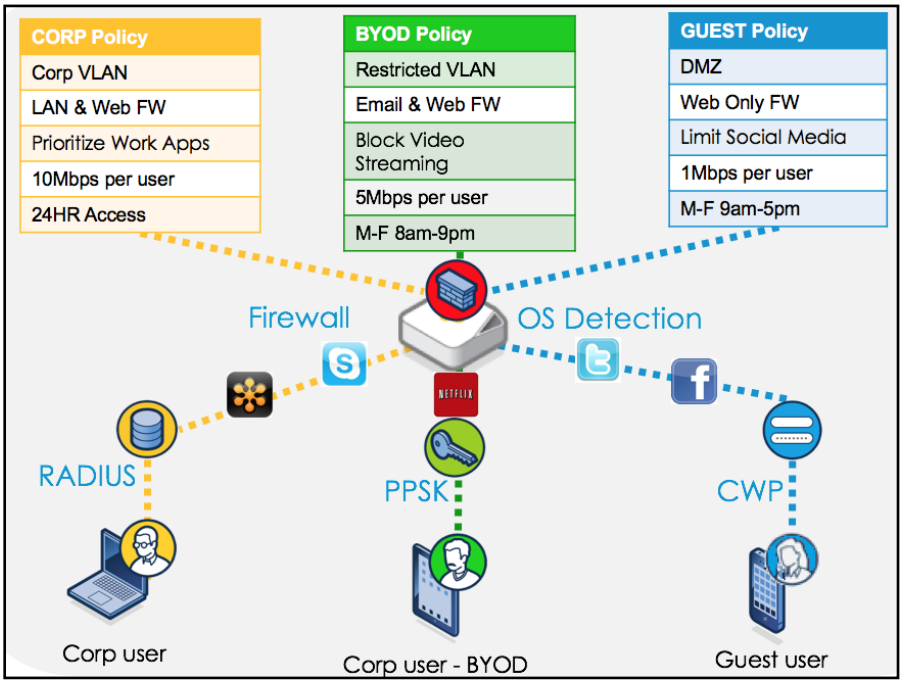



Figure 4: Policy based control

**(c) Standard: Workstation security**. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

Aerohive devices can be configured to support both wired and wireless 802.1X, which ensures that even wired devices can be prevented from accessing network resources without valid login credentials.

4 http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=b6bd13b5b652fe09e86dd86c442ee-b62&n=45y1.0.1.3.79&r=PART&ty=HTML#45:1.0.1.3.79.3.27.5

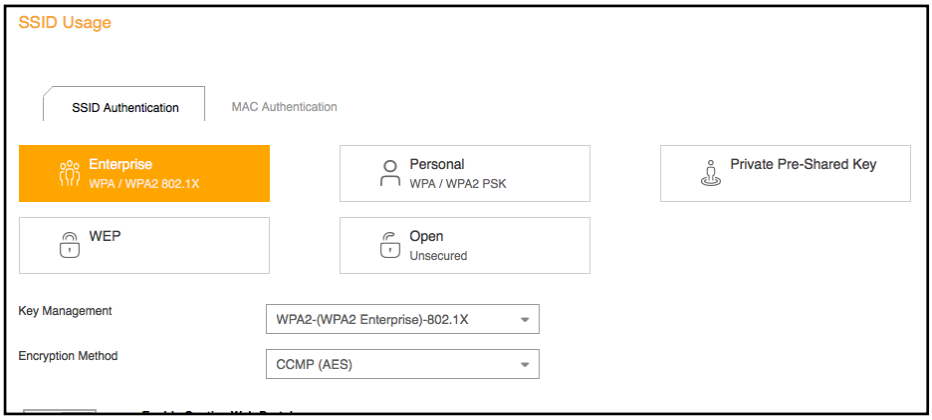



Figure 5: Unified device management

**(d)(1) Standard: Device and media controls.** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

Aerohive access points support locationing using any three Aerohive access points that can triangulate the position of connected clients or rogue access points. In addition, Aerohive can send information to AeroScout, Ekahau, or other RFID location vendors that use the Tazmen Sniffer protocol. This technology will allow an administrator to track the position of connected devices on the topology maps and even set alerts if devices are removed from specific areas.

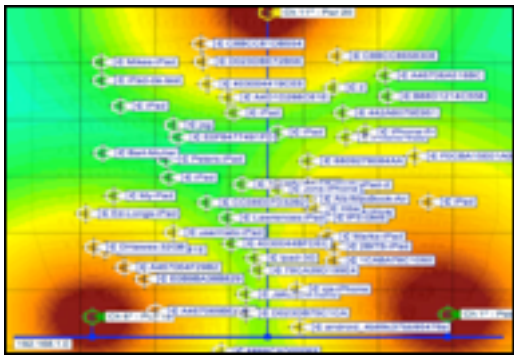


Figure 6: Device control and locationing

**(iii) Accountability (Addressable).** Maintain a record of the movements of hardware and electronic media and any person responsible therefore

In addition to the locationing capability listed above, client movement throughout the network is tracked in the HiveManager client logs to detail exactly which access points clients roam to as they move throughout the network.

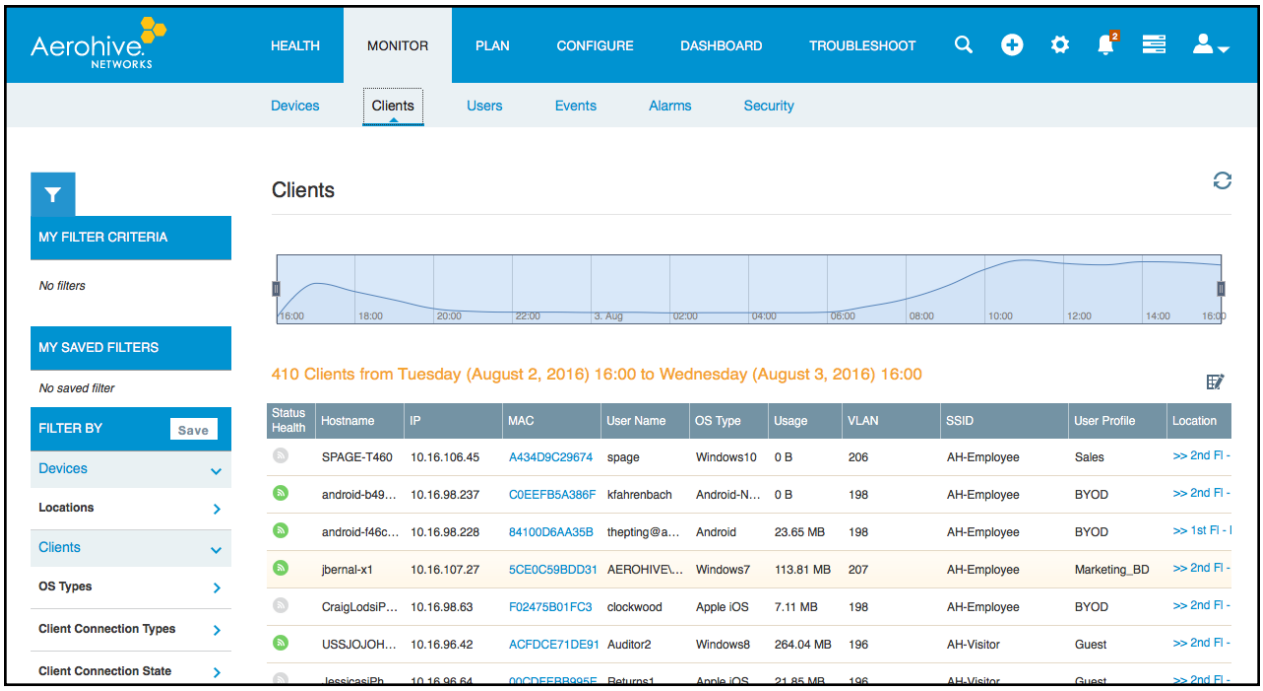



Figure 7: Clients logs and monitoring

## § 164.312 Technical safeguards[5]

**(a)(1) Standard:** Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

**(i) Unique user identification (Required)**. Assign a unique name and/or number for identifying and tracking user identity.

Aerohive supports several ways to identify users connected to the network. Aerohive devices support WPA2-Enterprise (802.1X) authentication, which requires the clients to authenticate against an authentication server, such as RADIUS, with a username/password or certificate. The Aerohive devices themselves can actually operate as RADIUS servers if needed, and join directly to a user store such as Active Directory, Open Directory, eDirectory, or LDAP. Aerohive devices also support Captive Web Portal with authentication, which requires a client to provide user credentials on a splash page before accessing the network. In addition, Aerohive devices support the Private Pre-Shared Key functionality, which allows an administrator to assign a unique access key to a specific user or device. This feature provides the benefit of unique encryption and authentication per end-point that is available with 802.1X, but does not require the use of certificates or an external authentication server.

Once the devices are securely connected to the network and the users are uniquely identified, extensive audit logging and reporting is available within HiveManager to detail client use on the network. Administrators can get a full history of client activities, including application visibility and controls. Reports can be scheduled and emailed directly from the HiveManager to ensure ongoing compliance.

5 http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=b6bd13b5b652fe09e86dd86c442ee-b62&n=45y1.0.1.3.79&r=PART&ty=HTML#45:1.0.1.3.79.3.27.6

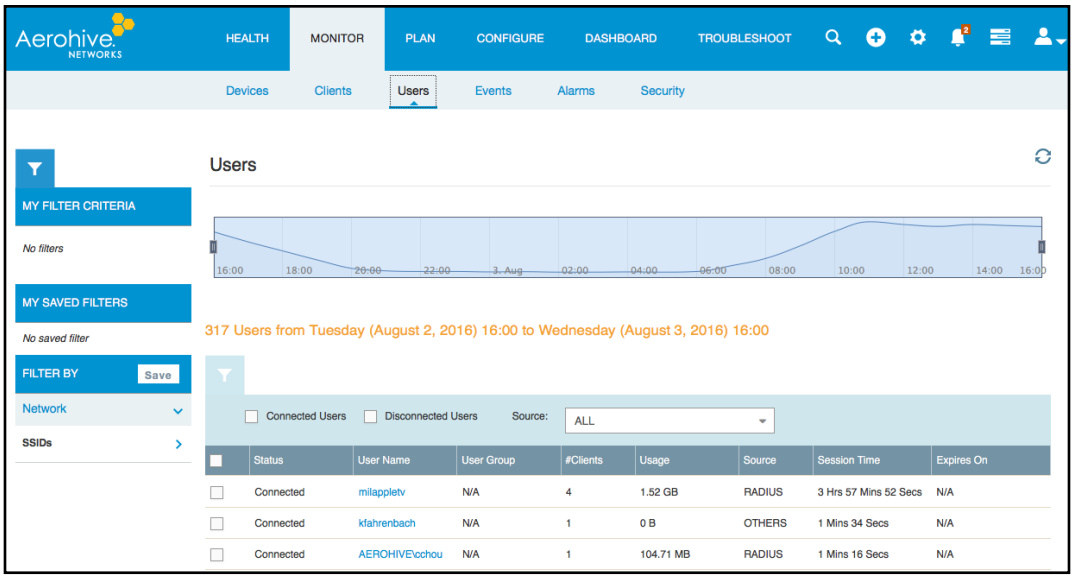



Figure 8: User monitoring log

**(ii) Emergency access procedure (Required)**. Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

Aerohive cooperative control is a fully resilient and redundant architecture. There is no single point of failure, and devices will continue to operate as normal even in the event of a WAN failure. Even if access to HiveManager is lost, devices can continue to log information to an external syslog or SNMP server, and Wi-Fi operations remain unaffected by loss of access to HiveManager. If the access points operate as RADIUS servers connected to an external user store, the access points can even cache user authentication information to allow for continued user authentication until the user store access is available again.
In addition, Aerohive branch routers (including the AP330 and AP350 in branch router mode) support USB modems for WAN connectivity. In the event of a catastrophic WAN failure, emergency connectivity can be provided via the USB modem. An administrator can even configure identity-based routing policies that restrict which users/devices can forward traffic over the USB connection.

**(iii) Automatic logoff (Addressable).** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Aerohive devices can easily be configured to terminate client access after a specified amount of time. Administrators can also manually de-auth a connected client right from the HiveManager interface.

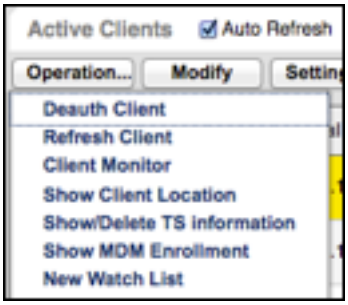
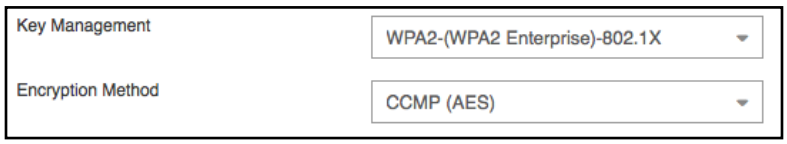



Figure 9: Session monitoring

**(iv) Encryption and decryption (Addressable).** Implement a mechanism to encrypt and decrypt electronic protected health information.

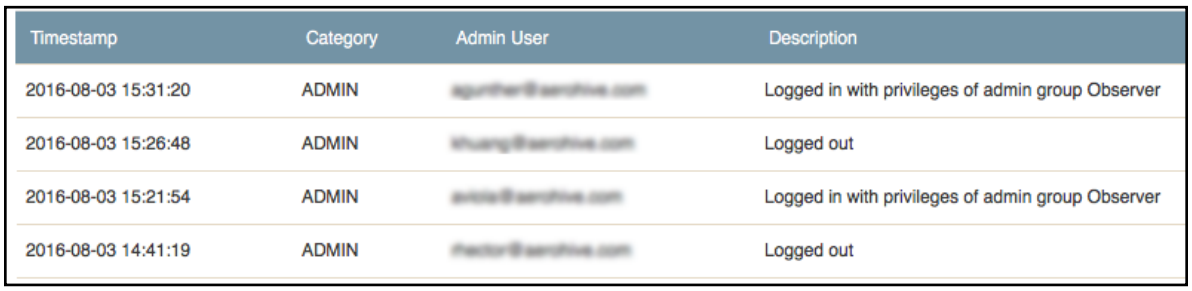
As far as transmitted data is concerned, Aerohive devices support WPA2-Enterprise with AES encryption (256 bit). Communication between the Aerohive devices and HiveManager is

conducted via DTLS (Datagram TLS).




**(b) Standard: Audit controls.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Extensive audit logging controls are available within HiveOS and HiveManager. All Aerohive devices support syslog to external logging servers, and most support SNMP to external logging servers. HiveManager can track all client information, including associations/de-associations, roaming, application usage, and bandwidth utilization to name a few. Historical information can be retained for configurable periods and exported via csv or pdf via download or email.



| Timestamp | Category | Admin User | Description |
|---|---|---|---|
| 2016-08-03 15:31:20 | ADMIN | [redacted] | Logged in with privileges of admin group Observer |
| 2016-08-03 15:26:48 | ADMIN | [redacted] | Logged out |
| 2016-08-03 15:21:54 | ADMIN | [redacted] | Logged in with privileges of admin group Observer |
| 2016-08-03 14:41:19 | ADMIN | [redacted] | Logged out |

Figure 10: Audit controls

**(c)(1) Standard: Integrity.** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

This particular standard does not apply to the wireless network directly, but Aerohive devices can be configured to use the built-in stateful firewall functionality to permit or deny access to specific clients based on identity, device type, location on the network, or time of day, and the devices can log access information to ensure ePHI is restricted.

**(d) Standard: Person or entity authentication.** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

This requirement can be met by using a form of authentication for the connecting users, such as 802.1X, PPSK, or CWP. 802.1X with certificates would assure the identity and device of the connecting client.

## Summary

Healthcare is an ever-changing and consistently challenging environment for technology, but Aerohive has a unique focus on ensuring the wireless LAN and access layer are easy to deploy, configure, manage, and monitor. Regardless of where you live around the world, technology is going to continue to play a larger and more critical role in healthcare, and it is important to stay informed and in compliance with all regulatory compliance requirements.

For more information on building a compliant network using Aerohive products, please contact us at +1-866-918-9918, email info365@aerohive.com, or check out our website at http://www.aerohive.com/solutions/industry/healthcare.html.

## About Aerohive

People want to work anywhere; on any device, and IT needs to enable them -- without drowning in complexity or compromising on security, performance, reliability or cost. Aerohive's mission is to Simpli-Fi these enterprise access networks with a cloud-enabled, self-organizing, service-aware, identity-based infrastructure that includes innovative Wi-Fi, VPN, branch routing and switching solutions.

Aerohive was founded in 2006 and is headquartered in Sunnyvale, Calif. The company's investors include Kleiner Perkins Caufield & Byers, Lightspeed Venture Partners, Northern Light Venture Capital, New Enterprise Associates, Inc. (NEA) and Institutional Venture Partners (IVP). For more information, please visit www.aerohive.com, call us at 408-510-6100, follow us on Twitter @ Aerohive, subscribe to our blog, join our community or become a fan on our Facebook page.


**Corporate Headquarters**
Aerohive Networks, Inc.
1011 McCarthy Blvd
Milpitas, CA 95035

Phone: 408.510.6100
Toll Free: 1.866.918.9918
Fax: 408.510.6199

info@aerohive.com
www.aerohive.com

**International Headquarters**
Aerohive Networks Europe LTD
The Courtyard
16-18 West Street
Farnham
Surrey, UK GU9 7DR

Phone: + 44 (0) 1252 736590
Fax: + 44 (0) 1252 711901