# HIPAA Standards and Wireless Networking

The Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress and has been in place since 1996. Although the act was primarily designed to aid and simplify portability of healthcare information, provisions were put in place to ensure the patient's right to privacy in the process.

This act has changed many of the methods and practices exercised by health care institutions nationwide. While some of these practices for protecting confidential physical records may be more obvious, the introduction of electronic media can make the task more complex. Complicating things further, the HIPPA act does not specify guidelines to ensure compliance. The rapidly changing nature of information technology makes managing this problem even more problematic.

## *The risks of the ordinary wireless LAN*

The risks of managing and maintaining paper records are considerable. Maintaining control of confidential records, but still providing easy access to those individuals that require the data is a fine balance. Information technology promised to provide a solution to this problem. Records could be protected and encrypted centrally, while health care professionals could access them remotely from a secure and password protected console. The problem with this solution is that healthcare professionals are, by their nature, extremely mobile.

The solution to this problem is wireless technology. However, with wireless networking systems, even greater care must be devoted to ensuring the security and privacy of patient data, as wireless networks bypass many of the physical security measures counted on by the health care professionals. No longer would someone need to trespass into a records room, or walk behind a station to have access to the network; it could be someone sitting in the parking lot.

Without proper security, valuable and private records could be accessed, networks could be compromised. Even with no malicious intent at all, people introducing equipment from home (like a low cost access point) may introduce a gaping hole in the network's security defenses.

Proper security must be designed in; it must not be an afterthought.

## What does complying with HIPAA mean?

Although HIPAA does not specify architectural guidelines or design considerations, it does make it clear that certain standards for security should be developed and enforced and that certain security elements must be considered in order satisfy HIPAA security guidelines. The cornerstones of these elements include Access Control (limiting who has access to what information), Authentication (validating users), Integrity Controls and Encryption. Unfortunately, these are often the weak spot of ordinary wireless networks.

In addition to these, they also mention Alarms, Audit Trail, and Event Reporting. The only way to ensure HIPAA compliance is to make sure that you have provided for each of these security elements when deploying your wireless network, and are considering your security policy.

> "Communications/network controls (If communications or networking is employed, the following implementation features must be implemented: Integrity controls, Message authentication. In addition, one of the following implementation features must be implemented: Access controls, Encryption. In addition, if using a network, the following four implementation features must be implemented: Alarm, Audit trail, Entity authentication, Event reporting)."
>
> *HIPAA - 45 CFR Part 142*
> *Security and Electronic Signature*
> *Standards; Proposed*

## Aruba: An Integrated Solution

Minimally, your wireless strategy must address all of these elements in order to ensure the security required by HIPAA. Optimally, these elements would be tightly integrated in order to provide a seamless security net throughout your network

**Encryption:** Although wireless offers many solutions for encryption, modern encryption techniques such as 802.1x and WPA2 provide unparalleled security. Although support for these standards on desktop devices is common, simultaneous support for alternate standards for other devices such as PDAs and VoIP handsets is preferable. Aruba allows these different encryption methods to cooperatively coexist, while still protecting your network with safeguards that prevent less secure devices from accessing inappropriate resources. In addition, Aruba also supports VPN technologies such as PPTP and IPSec

**Authentication:** Aruba integrates your choice of existing authentication methods, such as Windows Active Directory Server, LDAP or Radius servers with the previously mentioned encryption technology. This way, the same single login identity that allows

them to access your network's resources can be utilized to permit or deny access to the wireless LAN.

**Access Control:** Access Control also integrates tightly with Authentication and Encryption technologies in the Aruba Framework. Aruba's integrated stateful firewall prevents unauthorized access, and users identity and credentials can be used to permit or limit access to sensitive network resources. Powerful ACLs can be used to for ultimate control over who has access to which resources.

**Integrity Control:** Aruba's Self Healing Networking ensures the highest quality network connection and end user experience. Automatically calibrating networks choose optimal power and channel assignments, and automatically correct issues such as RF interference and network failures in order to guarantee the availability of your mission critical wireless applications.

**Alarms:** The Aruba Wireless system also incorporates a powerful Intrusion Detection System that proactively searches for wireless threats and helps to isolate them. Our rogue AP detection identifies unauthorized wireless LAN equipment functioning on the system, and can remotely disable the access point, eliminating the security breach. Hackers identified by the system can be placed in a "blacklist" to prevent this user from having any access to system resources.

**Audit Controls and Event Reporting:** The Aruba System has a flexible and powerful system logging mechanism to log network, system and user events, either internally or to an external Syslog server. This way, events such as user logins and associations, alarm logs and alerts, and network events such as device downtime can be logged and tracked for reference.

It is not enough to just have a loosely coupled solution to provide network security. Only by providing a tightly integrated and systemic approach to network security can you be assured of the integrity of your network and its valuable assets.

## *Conclusion*

The world has changed, and the modern IT environment reflects these changes. As a result, the health care industry has been mandated with maintaining the security of its patient's most valuable information. At the same time, wireless technologies promise to improve the world of the health care professional and in turn, improve the physician – patient relationship. Only Aruba Wireless Networks provide this rock solid security while still offering the freedom of the wireless network.

Aruba Wireless Networks
1322 Crossman Ave
Sunnyvale, CA 94089