
Jody Barnes

East Carolina University
Abstract

The use of wireless data networks in hospital environments offers effective and efficient communication but also poses many security considerations directly related to protecting Patient Health Information (PHI). In this paper we will look at the Physical and Technical Safeguards addressed by the Health Insurance Portability and Accountability Act (HIPAA) and the steps that can be taken to ensure they are met. We will also look at steps that can be taken to make the wireless data network HIPAA compliant. A list of best practices for wireless networks in hospital environments will be presented. Although wireless and HIPAA bring about new security concerns, if the correct steps are taken, a HIPAA compliant wireless network is possible.

HIPAA Overview

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was enacted to protect health information by establishing transaction standards for the exchange of health information, security standards, and privacy standards for the use and disclosure of individually identifiable health information. Entities directly impacted by this act are health plans, health clearinghouses and healthcare providers (“TLC HIPAA Overview”, n.d.).

Although there are other rules incorporated in HIPAA, the Security Rule has the most direct impact on hospital technology systems including network infrastructure. This rule addresses security measures such as user authentication, access controls, audit trails, controls of external communication links and access, physical security, systems back up, and disaster recovery. With increasingly more information being stored and transmitted electronically, the Security Rule works to identify and regulate these activities (Gue, n.d.).

Another major aspect of HIPAA is the Privacy Rule. The US Department of Health and Human Services (2003) states that “a major goal of the Privacy Rule is to assure that individuals’ health information is properly protected while allowing the flow of health information” (p. 1). This rule directly impacts the technology aspect of healthcare organizations due to more information being stored and transmitted electronically. However, the information must be protected allowing unproblematic access for those providing healthcare services.

April 2005, was the date for healthcare organizations to be HIPAA compliant. The only exception to the rule is for small institutions with less than $5 million in revenue. These
institutions have been given one additional year to become compliant. Those not in compliance with HIPAA face violations which can carry up to a $250,000 fine and jail time up to 10 years (Mercuri, 2004). Now is the time to be sure that existing and future practices and technologies are up to HIPAA standards.

HIPAA Standards

There are no specific criteria that make a network infrastructure, wireless or otherwise, HIPAA compliant. It is by purpose that the standards do not address specifics. It is expected that affected entities assess the security risk it faces and design, implement and maintain security to mitigate those risks. In other words, an organization is to look at its unique environment and determine where and if the HIPAA standards apply (Airespace, 2004). Once this is done, the organization is to use appropriate security procedures to reduce or eliminate these risks. Although the legislation is there for a guideline, it falls on the organization to determine what is appropriate for their specific situation.

The specific areas of HIPAA that should be considered when designing a wireless data network for a hospital fall into 2 major areas:

1. Physical Safeguards
2. Technical Safeguards

In the HIPAA Security Series, the Centers for Medicare and Medicaid Services (2005) give the following definitions. Physical Safeguards are defined as “physical measures, polices, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environment hazards, and unauthorized access” (Topic 3, p. 2). Secondly, Technical Safeguards are defined as “the technology and the policy and procedures for
its use that protect electronic protected health information and control access to it” (Topic 4, p. 2). These areas must be addressed when planning a wireless deployment in a hospital to show that clear and reasonable security measures are assessed and implemented. According to Mercuri (2004), “compliance is neither simple nor straightforward” (p. 26).

All aspects of the Physical and Technical Safeguards do not have to be used when planning wireless. As stated by O’Doriso (2003), “in order to provide the highest security to a wireless network, the relevant regulations need to be extracted from the HIPAA document and interpreted for use in the scenario presented” (p. 3). The following are the standards that need to be considered when implementing a wireless network in a hospital environment.

1. Facility Security Plan (162.310(a)(2)(ii)) to secure equipment from unauthorized physical access, tampering, and theft.

2. Access Controls (164.312(a)(1)) is basically who is granted access to resources.

3. Audit Controls (164.312(b)) is logging who, when, and where resources are accessed.

4. Integrity (164.312(c)(1)) is to assure that electronic PHI is protected from improper alteration and/or destruction.

5. Person/Entity Authentication (164.312(d)) is to assure that a person or entity trying to access information is the one claimed.

6. Transmission Security (164.312(e)(1)) is to ensure that information is kept private while being transmitted.

This is not a complete list of standards but only those to be used in designing a HIPAA compliant wireless data network. Many of the other controls can be implemented at other layers of the system and therefore are not going to be implemented in the wireless security layer. Once
again, HIPAA leaves interpretation to the individual organization; therefore you will ultimately decide whether this is a complete list for your setting.

Control Implementation to Meet Standards

There are many different approaches that can be taken to arrive at HIPAA compliance in a wireless setting. The following sections will look at ways to meet the previously mentioned standards. Again, this is only a few approaches and does by no means exhaust the possibilities that could be used.

Facility Security

Although most of the Physical Safeguards can be addressed at different locations in the hospital environment, the equipment protection component of Facility Security can be addressed within the wireless network. Two pieces of equipment that can be directly impacted by this control are the Wireless Access Point (WAP) and the devices used to access the wireless network such as laptops. If stolen or compromised, this equipment may be able to reveal aspects of the infrastructure that would compromise other security procedures put in place, such as encryption keys, access servers, IP schemes, etc. By protecting the equipment, you are protecting the information that it stores.

One way this can be addressed is with Radio Frequency Identification Tags (RFID). Although this technology is new and not readily available to everyone, it could be very useful. By attaching an RFID tag to the user device, an alarm sounds when the device leaves the intended area ("Airespace Wireless", n.d.). This would assist in asset control and insure the devices are not taken off hospital premises.
The physical security of the WAP also needs to be considered. Even though newer technology is going to “Light Weight Access Points (LWAP),” most WAPs in place now carry information that could be useful to an attacker. If the WAP were to be stolen and comprised, the entire network could be placed in jeopardy. Typically in a hospital environment, WAPs are in locations that are available to the public (“Airespace Wireless”, n.d.). One way to control physical security of the WAPs would be to have monitoring devices notify staff when a WAP goes offline. Staff could then respond to ensure the device has not been compromised. Although this is not a complete solution, earlier notification provides a more rapid reaction and response by staff.

There are many other aspects of security that need to be considered in a hospital wireless network, such as facility security. As mentioned by Grunman (2005), “in many organizations, the security focus tends to be on protecting the information as it travels through the network” and consideration is not given to the security of the network itself. The equipment being protected is in itself valuable, but it is the information stored on it that is most important.

Access Controls

Access controls are to provide the users with access and privileges to specific resources. In this case, the resource being protected would be the wireless network. Wireless Local Area Networks (WLANS) are inherently vulnerable because information is broadcast into the air where it is accessible to anyone with the right equipment and knowledge (Manley, M.E.; McEntee, C.A; Molet, A.M.; Park, J.S, 2005). “Depending on the location, environment, and facility construction, IEEE 802.11 signals can travel 150 to 1,000 feet” (Royster, 2005, p. 1). In
many cases wireless signals travel beyond the wall of the hospital, “Signal Leak”, access control must be considered both inside and outside of the institution.

One thing that can be done to help with the signal leak is the use of directional antennas. Although this will not eliminate radio signals outside of the facility, it can help limit it. This is something that should be considered during the design of the wireless network. It would be cost effective on a new install but would probably not be justifiable to replace antennas in an existing WLAN. Directional antennas are one small way to help prevent signal leak outside of the facility (O’Dorisio, 2003).

Another relatively simple step to limit the access to a WLAN is to disable Service Set Identifier (SSID) broadcast. Because client computers must present the correct SSID when associating to a WAP, this acts as a simple password and thus provides security (Dell, 2003). Although there is no security in obscurity, you shouldn’t advertise the WLAN to everyone, including potential attackers.

Access to the WLAN can also be limited based on the Media Access Control (MAC) addresses. This should only be considered for small environments where a MAC list can be efficiently managed (Dell, 2003). Another problem with MAC address filtering is that with the correct software, MAC addresses can easily be spoofed allowing an attacker to pose as a legitimate computer. As stated, MAC filtering does have problems, but in a small hospital environment with limited resources it may be an additional small defense option.

Physically and logically separating the WLAN from the wired network will help to separate network traffic and allow for security boundaries. If security is used on the gateway between the WLAN and the LAN, risk to resources residing on the wired network can be reduced. One way to accomplish this is by using a Virtual Private network (VPN) appliance between the WLAN
and the wired network, thus allowing traffic from authenticated users into the wired network. Another solution would be to use an Access Control List between the two networks allowing traffic based on such things as MAC address, IP Address, application, physical location and a host of other properties (Airespace, 2004). Physically and logically separating the wired and wireless data networks provides the ability to filter the traffic between the two adding another layer of Access Control.

A solution frequently used for Access Control is 802.1x. By using 802.1x, the user must be authenticated before access to the wireless network is granted. This means without the correct credentials, access will not be allowed. Although there are many more prevalent reasons to use 802.1x technology, it will help with HIPAA compliance in regards to access control (Cisco, n.d.).

Access control is not limited to, nor restricted by the procedures mentioned here. By itself, not one of these individual controls provides a complete solution. The idea is to layer the Access Control mechanism so you are not subject to the vulnerabilities of the mechanisms individually.

**Audit Controls**

Audit Controls are used to track and examine activity in information systems. This can be applied directly to WLANs. We need to know who accesses the WLAN and the resources they use while connected. There are number of approaches that can be taken with auditing a WLAN and here we will take a look at a few that would prove useful in the hospital setting.

If users are required to use a VPN connection to access the wired LAN from the WLAN, the VPN concentrator itself could be used for auditing. Most VPN appliances have the ability to log statistic, users, traffic, as well as many other aspects of network connectivity. Logging, if used
Wireless Data Network Security

correctly, could provide a very useful audit trail of user’s accessing the systems. All traffic entering the wired LAN would be required to travel through the VPN and therefore be logged. This is a control that should be used if a VPN connection is used as a gateway between the two networks. If a VPN is not used, there are other solutions that can be adopted for auditing (O’Dorisio, 2003).

A solution that could be used in the case where a VPN was not being used is an Intrusion Detection System (IDS). If the IDS is placed between the wired and wireless LAN, it can be used to log traffic between the two. In most cases, with the IDS you have the ability to establish the traffic you want to monitor. This would be beneficial if you use a guest account that will only access the Internet. In this case, you may not want the traffic to be logged. With IDS, you have flexibility as well as the means to stay HIPAA compliant.

Here we have shown two commonly used procedures for wireless traffic. By monitoring the traffic as it enters the wired infrastructure, you have the ability to maintain HIPAA compliance as longs as the PHI resides on the wired network.

**Integrity**

Integrity Controls are put in place to insure that data has not been altered or destroyed in an unauthorized manner (Centers for Medicare, Topic 4, 2005.). When considering wireless security and integrity, we must make sure that the data is not altered or damaged during transit over the WLAN. Many protocols have built-in mechanisms for integrity checks. Here we will look at a few ways that we can add another layer for checking the integrity of transmitted information.

If we revisit the VPN gateway solution, we see built-in abilities for integrity. Not only does the VPN provide strong encryption, which helps protect the data, it will check that the data has
not been altered. Depending on the vendor of the VPN gateway being used, different approaches may be used for the integrity check. Although different, most would be considered HIPAA compliant (O’Dorisio, 2003).

Another type of integrity check is included in Wi-Fi Protected Access (WPA). WPA has two protocols to help with integrity and confidentiality. The Michael message integrity check (MIC) helps to insure that a message has not been replayed or modified (Arbaugh, 2003). Another integrity check that could be deployed is Cisco Message Integrity Check (CMIC). Both of these checks help to insure that data has not been altered or damaged during transmission (Cisco, n.d.).

Although there are other ways to verify the integrity of data traveling over a WLAN, the above solutions are a few approaches that could be deployed. These methods in combination with standard protocol checks will help to meet integrity compliance while data is being transmitted over the WLAN.

**Person or Entity Authentication**

Authentication Controls must be put in place to assure that the person or entity trying to access the system, in this case the wireless network, is who they claim. Authentication is usually considered at the server level, but here we will look at authenticating the user as they gain access to the WLAN, thus adding another layer of security to help ensure HIPAA compliance (O’Dorisio, 2003). As Gruman (2005) states, “authentication is one of the trickier aspects of wireless security.”

If we revisit our VPN solution once again, we find that we have the ability to provide authentication controls as the user tries to gain access to the wired network. For a person or entity to access PHI stored on the wired network, they must authenticate through the VPN to
gain access. This helps to make certain that the person or entity that tries to access resources on the wired LAN and already been authenticated once.

Another way to provide authentication control is to require the user be authenticated before being allowed to connect to the WLAN. By using framework defined by IEEE 802.1x standard, a WLAN can support centralized authentication. This centralized authentication can be done through a central authentication such as a Remote Authentication Dial-in User Service (Radius) server. Using 802.1x specifies use of Extensible Authentication Protocol (EAP) between the supplicant and authenticator (Cisco, n.d.). There are many different types of EAP that may be used, and any will help increase HIPAA compliance.

By using one of the previously discussed methods of wireless authentication, you will help guarantee that the person accessing PHI over the WLAN is in fact, who they claim. This will help to ensure the overall security and protection of resources within the hospital infrastructure.

*Transmission Security*

Transmission security, as it relates to HIPAA, requires that measures be taken to guard against unauthorized access of PHI while in transit over electronic communication networks (Centers for Medicare, Topic 4, 2005). Everything that is transmitted over the WLAN must be kept private. This can become a major priority since the media is the air (O’Dorisio 2003). We must focus on encryption to achieve compliance in this area.

One method for keeping data private during transmission goes back to our VPN solution. All traffic transmitted between the client and the VPN gateway is encrypted typically with Triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES). As mentioned by O’Dorisio (2003), “the key to keeping this (the VPN tunnel) secure though, is having strong
authentication at the firewall” (p. 9). If the authentication is reliable and strong, the transmission security is handled by the VPN.

When it comes to encryption, most have heard of the vulnerabilities of Wired Equivalent Privacy (WEP). To help address the vulnerabilities with WEP, things such as Temporal Key Integrity Protocol (TKIP) and Cisco Key Integrity Protocol (CKIP) are being adopted. These technologies both address the key management issues with WEP, as well as provide for per-session per-user keys (Cisco, n.d.). Both of the technologies would help to make sure that the data transmitted over the wireless network is secure. As a result of transmission security provided, the technologies also provide HIPAA compliance.

Another encryption method that can be used for transmission security is Advanced Encryption Standard (AES). AES overcomes the vulnerabilities of WEP but is typically not backwards compatible with many older clients. So if the WLAN will be a new install, AES should definitely be considered as the encryption method (Cisco, n.d.).

When it comes to encrypting data that is traveling on WLAN, some encryption is better than none. As stated by Manley et al (2005), “a rather obvious, yet dangerous security issue is that many network administrators never bother to properly configure WAPs connected to their networks” (p. 151). This not only makes the device itself very vulnerable, but also the information that it transmits. Although there are flaws with some existing technologies such as WEP, even vulnerable security is better than no security.

Conclusion

When implementing wireless data network security to comply with HIPAA regulations, many different approaches may be taken. You may consider a VPN solution that covers all HIPAA...
requirements or you may decide to build your security in pieces. No matter which actions you take, one thing is certain “wireless networks will never be one hundred percent secure, nothing will every be one hundred percent secure” (O’Dorisio, 2003, p. 10). What we must do is assess the individual hospital, formulate a plan that covers all addressable areas, and then monitor our solutions to ensure that they perform as we anticipated. As with other types of security, a wireless network security policy is also critical in the success of a secure wireless environment (Hagland, 2004). Although there is often a trade-off between WLANs and security, if enough thought and consideration is given to the project, a secure HIPAA compliant WLAN is possible.
References


