Global Information Assurance Certification Paper

Implementing A HIPAA Compliant Wireless Network

Sans Security Essentials Practical Assignment

Lynda Moore – Version 1.4b. Option 1

Table of Contents

Introduction

Wireless deployment provides a hot topic for the medical community these days. Recent articles in the health news indicate many uses for wireless networking or Wi-Fi (abbreviation for wireless fidelity). Immediate access to patient records from any location via a wireless connection leads to increases in quality of care while easing the burden on busy physicians and nurses. [22][21] Wireless networking in the health settings speeds admissions and insurance certifications for hospital stays and treatments. [20] Wireless networking can also offer better workflow and savings in installation and maintenance cost over conventional wired network. [22]. No one argues that Wi-Fi can substantially benefit the medical community; but there is much discussion if wireless networking can be made secure enough to satisfy HIPAA requirements. And HIPAA requirements are just the beginning of the problems that can occur if inappropriate access to personal health information is allowed. There may be class action lawsuits, as well as loss of reputation following theft of health information. [10]

This paper proposes to identify and discuss the portions of the HIPAA regulations that are relevant to wireless networking; and show how wireless networking can comply with these regulations.

Health Insurance Portability and Accountability Act Overview

In 1996 the president signed the Health Insurance Portability and Accountability Act (HIPAA). It was written for two main purposes. The first was to assure the portability of health information. The portability portion standardized a set of formats used to exchange information between health care providers and insurance suppliers. The second main purpose of the bill was to assure the privacy of health information. They proposed a rigid set of standards to protect the privacy of patient information from both inadvertent disclosure during routine daily operational use and intentional disclosure, such as sharing health information with pharmaceutical companies. These standards were further broken down into privacy standards and security standards.

The Privacy Rule has been published since 2001 and, since April 14, must be complied with by health plans, healthcare clearinghouses and health care providers (collectively know as covered entities). It is applicable to all protected health formation (PHI) in either paper or electronic form. It set standards for how the PHI may be used and disclosed – basically who the entity can give the PHI to and for what purpose. [13]

The Security Rule was published in February of this year. Entities have until April 2005 to comply with the standards set forth in the rule. The rule is divided into administrative safeguards, physical safeguards, and technical safeguards. Each of the safeguards have a set of standards that implement the safeguard. These

standards are either required or addressable. The addressable safeguards may be implemented as specified by set of parameters that include; determinations of entity size, infrastructure and capability, cost, and probably/criticality of risks [11]. The Security Rule also notes that these standards are the minimal that an entity should implement to comply with the rule. Local regulations may specify more.

Wireless Networking Security

The wireless networking protocol specified by the IEEE is 802.11. The Wired Equivalency Protocol Security (WEP) implements security for wireless data transmissions. WEP was designed, as the name implies, to provide 802.11 transmissions with the same security that wired transmission enjoyed. WEP goals were to 1) preserve the integrity of the data by sending an integrity check vector (ICV) along with the data. This ICV is computed by performing a CRC-32 on the original frame, and 2) preserve the confidentiality of data during transmission by encrypting the data plus the ICV using utilizing a symmetric key encryption scheme – RC4. [15]

Unfortunately in 2000, a flaw was found in the WEP algorithm. It was found to be possible to crack a WEP key with a little as a million packets. [6]

Complying With HIPAA

The final security rule released in February of this year showed a substantial change from the proposed security rule published in 1998 by eliminating specific implementation features to 55 technical standards [13]. This allows the security rules to remain relevant in the face of rapid technological advancement.

Administrative Safeguards

Implementation of Wi-Fi under HIPAA requires you look at all sections of the Security Rule. This includes looking at the administrative safeguards of risk assessment, risk management, and the policies and procedures governing use.

Risk Analysis

Risk analysis or assessment is a required implementation of the security management process standard and can be defined as the identification of 1) threats and vulnerabilities and 2) the potential impact a loss of data confidentiality, integrity or availability would have on the entity. [2]

Assessing risk involves knowing what threats are integral to wireless deployment and identifying your vulnerability to each threat. Common threats to wireless implementations include:

1) Denial of service (DOS) attacks are initiated to prevent access to the network. Wireless LANs (WLAN) are subject to several methods of DOS. An attacker can create a device that produces noise at 2.4 GHz effectively jamming the band. A rogue access point could broadcast a false SSID luring Wi-Fi clients into associating incorrectly and then monitor or save all traffic from the hapless client. An attacker could associate with an access point and then send floods of traffic such as an ICMP flood to overwhelm the wireless network [19].
2) Man-in-the-Middle-Attacks (MITM) can consist of either eavesdropping attacks where an attacker listens in on the wireless network and collects data or eavesdropping plus manipulation of the data. Manipulation of emails or database transactions can occur when an attacker, using ARP poisoning, imitates another client on the network [19].
3) Illicit use occurs when an attacker uses the wireless network to connect to other networks such as the Internet. Uses of an illicit wireless connection include sending spam, hacking local servers, hacking other networks or just defying onerous network rules [19].
4) Theft or loss of wireless portable devices could result in compromise of patient data on the device. Saved passwords and encryption keys could allow unauthorized access into the network and applications [14].
5) Physical compromise of access points could allow an attacker to easily launch DOS and MITM attacks.

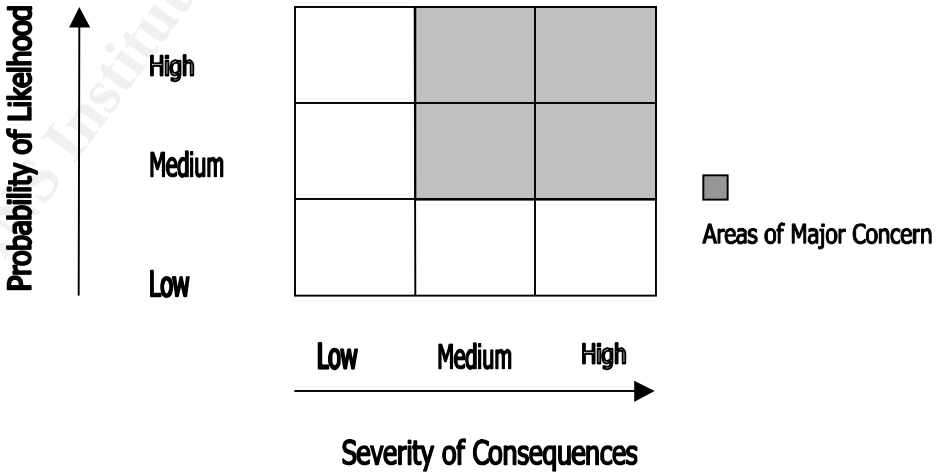
Assessing vulnerability involves looking at your wireless implementation and determining the extent to which each threat is mitigated by the controls of your wireless deployment. You will be looking at the probability that a threat connects with its corresponding vulnerability. You should note what control you have in place and if there is an adequate level assurance that the implementation is performing it's function. [2]

1) Decide what controls you have in place to mitigate the risk posed by DOS attacks. Do you control location of access points that make them difficult to access? Do you limit the information broadcast by the APs making it difficult for an attacker to associate? Do you have a firewall between your wired and wireless network to control traffic types? Do you monitor your network for unknown MAC addresses that might indicate a rogue access point? Do you monitor your access points for approved configurations? Do you have approved configurations?
2) Discover what controls diminish the possibility of MITM attacks. Realize that controls that limit the probability of DOS attacks also limit MITM attacks. Do you require WEP at the very least? Do you require Wi-Fi Protected Access (WPA) or a proprietary solution to the problems of WEP? Do you encrypt your database transactions? Do you encrypt email? Do you limit access to the wireless network to VPN connections only?

3) Ascertain what controls restrict illicit use of the wireless network. Controls that make it difficult to associate with an AP hinder illicit use. Do you require authentication of both the client and the access point? How many factors are involved in the authentication?
4) Determine the controls in place to limit risk should a portable wireless client fall into the hands of an attacker. Are all devices password protected? Is sensitive data on portable devices required to be encrypted? Is virus checking employed?
5) Find out if APs can be physically compromised. Are locations of APs documented? Are locations of APs limited by policy to certain locations? Who may install APs – IS personnel or anyone?

Now that openness of vulnerabilities to threats has been identified you need to perform the second component of risk analysis – determining the potential impact a loss of data confidentiality, integrity or availability. What kind of data flows over your wireless network? Is this the only access to this specific data? Data flow in the medical environment can contain information such as patient financial data, patient health data, institutional financial data, purchasing orders, etc. Loss of the confidentiality of purchasing orders would have a minimal impact while an eavesdropping attack that intercepted and published patient financial data would have devastating effects. Loss of integrity of helpdesk records wouldn't create the risk of a change in a patient's records. Loss of availability of email would not pose the problem of loss of the ability to order medical treatment.

To complete the risk assessment, you must evaluate the probability of a particular threat/vulnerability against each asset that will be vulnerable. One method appears in the GSEC manual [18].



A recent National Institute of Standards (NIST) publication attempted to specify a categorization of information systems by asking for a determination of level of risk that considered both threats/vulnerability and impact with a higher weight on

impact. [2]The categorization called for a determination of risk level for each of the security objectives of confidentiality, integrity and availability. Risk levels were specifically defined to be:

1) Low-loss would be expected to cause negative outcome or result in limited damage to operations.
2) Medium-loss would be expected to cause significant degradation in operational ability or result in major damage to assets
3) High-loss would be expected to cause catastrophic effect on operational ability or assets and loss of capability for a period that poses a threat to human life

A categorization of a physician order entry system might be as follows: [2]

CATEGORIZATION=[(confidentiality, medium), (integrity, high), (availability, low)]

Risk Management

Risk management is a required implementation of the security management process standard. It depends on the risk assessment previously performed. In determining the controls in place to mitigate threats, you were effectively looking at risk management that was in place. It is generally accepted there is no way eliminate all risk and still have functionality. So the goal of risk management is to reduce risk to a level that the entity can tolerate. HIPAA calls for entities to "implement security measures sufficient to reduce risks and vulnerabilities to an acceptable and appropriate level" [3]. Although the usage of "acceptable and appropriate level" is somewhat ambiguous, comments by the Department of Health and Human Services, attention to information security after the 2001 terrorist attacks and recent identity thefts have raised the bar on what "acceptable and appropriate" mean [11]. Basically this means that if you are transmitting patient information over your wireless network, you should have in place the best controls available, such a making VPN a requirement.

Managing risk is an ongoing effort. Once you have placed controls to minimize exposure to known threat/vulnerability duets, you must monitor the current state of affairs in the wireless world. New vulnerabilities are revealed daily. You must be prepared to reassess your controls to provide protection against any new threat.

Risk management should always follow the principles of defense-in-depth especially in the Wi-Fi arena considering the known flaws in the security implementation.

Policies and Procedures Governing Wireless Use

Many of the administrative safeguards specify the creation of policies and procedures to authorize and grant access to protected health information (PHI). In the case of wireless networking, we will focus on denying inappropriate authorization and access to PHI. Policies should state broad goals while procedures or guidelines should specify the details of implementing the goals.

Policy Specifications for Wireless Implementations

A security policy should 1) set the rules for expected behaviors by users, system administrators, management and security personnel, 2) authorize the monitoring, probing and investigation of systems and 3) define and authorize the consequences of a violation. [11].

A good security policy becomes one of the controls in place to help mitigate the risks involved in wireless networking. Return to the known vulnerabilities of Wi-Fi and craft your policies to address the associated risks. Policy wording should be general with details of implementation left to the procedures. Consider the following for policy inclusion depending on associated risk levels.

1) Take control of the WLAN. Specify that all network devices must be approved and configured to a set of standards. Ban unauthorized access points specifically. Owning control of the WLAN will limit your exposure to risks associated with the threats of DOS attacks, MITM attacks and illicit use.
2) Give authority for scanning of the wireless network. This permits IS personnel to look for violations of policy and therefore also controlling risks from DOS attacks, MITM attacks and illicit use.
3) Specify that portable devices connecting to the WLAN must have a minimal configuration that provides confidentiality to PHI that might be stored on the device. This reduces the risk associated with the loss of a portable device.
4) State the punishment for failing to comply with the policy.

Procedure Specifications for Wireless Implementations

Procedures spell-out the implementation details of the policies. Procedures should include who is responsible for executing the process, when the procedure should be used, and a frequency or timeframe if needed. There should be procedures to cover the configuration of access points, wireless network scanning and portable device configuration.

Delineate access point configuration procedures that include best practices for securing wireless network devices. [14] [5] [7]

1) Disable broadcast of SSID

2) Broadcast SSID at higher bandwidth and reduce the frequency of broadcasts
3) Change the default SSIDs and make non-standard
4) Enable encryption even if only WEP
5) Choose strong encryption keys and change frequently
6) Change default vendor passwords
7) Administer access points using SSH or HTTPS.
8) Use static IP addresses to make it difficult to get authorized even if associated
9) Require that access point firmware be current.
10) Require that access point placement be as far from outside walls as possible
11) Use MAC level filtering on access points to authorize who connects

Procedures for scanning your wireless network should provide methods to scan for access points that might allow unauthorized users. [7] [5] [8].

1) Scan WLANs for access point configuration to insure compliance and to spot access points that have had configurations changed illegally.
2) Scan WLANs for rogue access points. This can be done by sniffing wireless traffic for unapproved SSIDs or by the wired network sniffing for MAC addresses that are not in the database of allowed devices.
3) Scan from outdoors to determine signal strength outside the buildings.
4) Scans for web servers may show rogue access points.

Procedures for portable device configuration should take into account the intended use of the portable device. If PHI is to be stored on a device, strict configurations are required to prevent unauthorized access to the PHI if the portable device is lost. Required elements of portable device configuration would include: [14][20][4]

1) Install virus protection on all portable devices and keep it updated.
2) Protect access to portable devices via passwords minimally.
3) Install personal firewalls.
4) Encrypt data stored and containing PHI.
5) Disable password caching for applications.
6) Require WPA on all transmissions involving PHI and consider requiring VPN.
7) Consider requiring regular inspection of portable devices to assess compliance.
8) Determine ownership of portable devices. It may be that buying portable devices and loaning to users may be most secure method of allowing wireless access to network.

Physical Safeguards

The physical safeguard section of the Security Rule Specifies that entities should implement policies and procedures that limit physical access while ensuring that properly authorized access is allowed. [3] Implementation of this rule by Wi-Fi requires placement of access points that are not easily accessible and utilizing either WPA or vendor-specific combinations of strong authentication and encryption.

Technical Safeguards

The technical safeguard section of the Security Rule specifies technical procedures for access controls, audit controls, information integrity controls, authentication, and transmission security.

Access controls, audit controls, information integrity controls and authentication apply to data at rest and so must be applied information systems that manufacture or use PHI. Current wireless utilization is as a client for other information systems whether to enter PHI or view PHI for treatment purposes. Previously defined policies and procedures for portable device use specify protection for temporarily stored PHI.

For a wireless network to provide transmission security, it must ensure the integrity and encryption of electronically transmitted PHI. This fact is at the heart of many decisions to postpone wireless deployment until the IEEE releases a security extension to the 802.11 protocol that would replace WEP. [10] Others think that the delivery of healthcare is the first priority and if Wi-Fi can assist in the quality of healthcare, then it should be implemented. [16]

Fortunately it is not necessary to wait for implementation of 802,11i to for a HIPA compliant wireless network. There are several methods currently available that, used as extensions to WEP or replacing it altogether, make wireless networking comply with the security rules.

Virtual Private Networks

Virtual private networks (VPNs) have been used for several years to provide integrity, encryption and authentication to transmissions over wired networks. It provides integrity through encryption and can provide authentication via several mechanisms such as tokens. VPN utilizes the IPSec protocol to encrypt data before it is encrypted by WEP. Used with WEP, this prevents unauthorized examination of PHI even if the WEP key is compromised. Drawbacks to this approach are 1) need to install a client on each portable device, 2) problems with dropped services during access point re-association and 3) need for VPN gateway. [11] If VPN is already installed at an entity, requiring VPN access over wireless may be the best solution and would certainly be the quickest. Since it is

an accepted solution for wired networks, use of VPN would certainly present an "acceptable and appropriate" solution to WEPs problems with encryption and integrity.

WPA

By mid-year, it was expected that WPA would replace WEP as the wireless security protocol of choice. [1] While WPA is not an official IEEE standard, it is based on the upcoming 802.11i and should be compatible.

WPA consists of two components that improve on two downfalls of the WEP protocol by providing Temporal Key Integrity Protocol (TKIP) to alleviate key weakness and integrity issues; and adds support for authentication via Radius servers and Extensible Authentication Protocol (EAP). Solving these two problems make wireless networking compliant with HIPAA technology standards by increasing encryption strength and ensuring integrity of PHI and as a bonus add auditing capabilities by supporting strong authentication.

TKIP

TKIP is a set of algorithms that wrap WEP to increase security and are designed to be implemented on legacy hardware. [EE]. TKIP adds several strengths to WEP: [9][14]

1) TKIP specifies use of 48-bit initialization vectors (IV) instead of WEPs 24-bit IV. This results in a longer period between the reuse of IV and reduces the chance that a hacker can collect enough frames to deduce the encryption key. This strengthens the wireless
2) New encryption keys are automatically generated for each client connected to a WPA enabled station every 10,000,frames. Each frame also has a unique key. This avoids the same key being used long enough to break and additional protects against loss of data should one key be compromised.
3) Message integrity code (MIC) utilizes an 8-bit code called Michael to increase the integrity of wireless frames.

The addition of WPA to WEP makes it much harder for a hacker to eavesdrop on a wireless transmission and also decreases the chances that data will be manipulated. Risk assessment should be used to validate if the subsequent decrease in vulnerability reduces the risk of wireless networking using WPA "acceptable and appropriate".

801.1x

WPA also offers the option of authentication via pre-shared key or via RADIUS or LDAP server using Extensible Authentication Protocol. While not directly

contributing to compliance with the transmission security portion of the Security Rules, it provides for authentication of the access points and therefore increases the level of overall security by decreasing the possibility of MITM attacks.

The three main elements of the 802.1x and EAP approach include: [6]

1) Mutual authentication between client and authentication server via shared keys such as passwords or tokens
2) Encryption keys derived after authentication
3) Re-authentication and new encryption keys triggered automatically.

Access point authentication can occur via access control lists on the authentication server.

802.11i

The 802.11i extension to the wireless protocol is expected to be approved by early 2004. Main components are 802.1x along with TKIP with the addition of counter mode with CBC-MAC protocol (CCMP). [12] CCMP ensures data confidentiality as well as integrity and authentication. It also offers AES as an alternate encryption to RC4. [12]

Conclusion

Wireless networking in the clinical setting is a technology that can offer much value to an entity in the form of better patient care, increased ROI over wired networks, and decreased workload on physicians and hospital staff. The technologies to secure wireless networking to comply with HIPAA are already present. These technologies require careful planning and implementation to ensure an “acceptable and appropriate” level of risk to PHI but a risk assessment should indicate that wireless is ready for HIPAA.

[1] “Understanding the Layers of Wireless LAN Security and Management”, http://www.airdefense.net/whitepapers/paper_layers.shtm .

[2] “Standards for Security Categorization of Federal Information and Information Systems”, http://csrc.nist.gov/publications/drafts/FIPS-PUB-199-ipd.pdf.

[3] Federal Register, Volume 68, Number 34, Thursday, February 20, 2003. pp. 8376-8380. http://aspe.hhs.gov/admnsimp/FINAL/FR03-8381.pdf.

[4] Arora, Rakesh. “State of Affairs of Wireless Networks,” http://www.giac.org/practical/GSEC/Rakesh_Arora_GSEC.pdf.

[5] Chin, Tyler. “Why Wi-Fi? Getting a Better Connection”. http://www.ama-assn.org/sci-pubs/amnews/pick_03/bisa0414.htm

[6] Convery, Sean, Miller, Darrin, Sundaralingam, Sri. “CISCO SAFE: Wireless LAN Security in Depth”. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.pdf

[7] Geier, Jim. “The Guts of WLAN Security Policy”. http:// www.wi-fiplanet.com/tutorials/article.pnp/1489151.

[8] Geier, Jim. “Identifying Rogue Access Points”. http://www.wi-fiplanet.com/Tutorials/article.php/1564431.

[9] Geier, Jim. “WPA Security Enhancements”. http://www.WI-Fiplanet.com/tutorials/article.php/2148721

[10] Gainer, Randy, Van Eckhardt, Michael, Williams, Rebecca L., and Marks, R. “HIPPAA and WIFI – Regulatory Tangles for Wireless Healthcare Networks”. http://articles.corporate.findlaw.com/articles/file/00010/008895

[11] Gainer, R., Van Eckhardt, M., Williams, R.L., Marks, R.D. “Wireless Security Standards”. http://www.dwt.com/practc/hc_ecom/bulletins/05-03_BNAarticle.htm

[12] Hamid, Radidah Abdul. “Wireless LAN: Security Issues and Solutions”. http://

[13] Jinnett, Jeff. “Overview of the Final HIPAA Security Rule”. http://www.ebglaw.com/article_784.pdf

[14] McDonough, Claire. “Identifying the Risk Involved in Allowing Wireless Portable Devices Into Your Company”. http://www.giac.org/practical/GSEC/Claire_McDonough_GSEC.pdf

[15] Menta, Princy C. "Wired Equivalent Privacy Vulnerability". http://ouah.kernsh.org/wirelessvuln.htm

[16] Walker, Jesse. "802.11 Security Series". http://cedar.intec.com/media/pdf/security/80211-partz.pdf

[17] Vaughn-Nichols, Steven J. "Making The WPA Upgrade". http://www.wi-fiplanet.com/tutorials/article.php/2201281.

[18] Cole, E., Fossen, J., Northcutt, S., Pomeranz, H. SANS Security Essentials with CISSP CBK. SANS Press, February 2003. p831.

[19] Potter, B., Fleck B. 802.11 Security, Sebastopol: O'Reilly, December 2002. pp 18-29.

[20] "Mercy Medical Center Improves Efficiency and Quality with Wireless LAN Technology". http://www.wlana.org/ent/user/mercymed.htm

[21] "Saint Joseph: Wireless LAN Helps Hospital Meet Managed Health Care Challenge". http://www.wlana.org/ent/user/stjoe.htm

[22]"Austin Regional: Wireless-Linked Computers Speed Billing at Medical Clinics". http://www.wlana.org/ent/user/austmed.htm