RUNNING HEAD: Securing the E-mail System

Information Security: Securing the E-Mail System in the Healthcare Organization

Karen R. Watson

DTEC 6823

watsonk@ecu.edu

Publication date: July 20, 2007 at http://ww.infosecwriters.com

Autobiographical Notes

Karen Watson

Karen Watson is a Technology & Support Analyst at East Carolina University. She has worked in the Information Systems: Network Administration field for 5 years in Eastern North Carolina. Karen began working in networking in 2002 at WNCT-TV9 after graduating from the Networking Program at Pitt Community College. Karen was Cisco Certified Network Associate in 2002 and certified as a CompTia Network + Certified Professional in 2005. Karen also obtained an undergraduate degree in Business Administration from Barton College in Wilson, NC. Karen continues to work in the Information Systems and business administration fields.

.

Abstract

Today an e-mail system can be a vital business tool in the health care organization. The health care organization use e-mail to conduct business with a business associate pertinent to the daily operations of the health care organization. The business associate normally signs a Business Associate Agreement (BAA) for a health care organization for the purposes of the security of the electronic health information. Even though the BAA exists, there are still potential glitches, threats, and vulnerabilities within the e-mail system and among the users, which can cause a breach of the electronic information. Therefore, the security of the e-mail system is necessary, but the privacy of an employee's e-mails may also be necessary according to the Electronic Communications Protection Act (ECPA). More importantly, the security, confidentiality, integrity, and availability of Electronic Protected Health Information (EPHI) are mandatory according to the legislative guidelines of the Health Insurance Portability and Accountability Act (HIPPA). The research paper presents the uses of the e-mail system in a health care organization, the challenges of the e-mail system in the heath care organization and the preventative actions necessary to secure the e-mail system in the healthcare organization. Under the privacy challenge, the legal issues, which may arise from the misuse of the EPHI in the health care organization, will be presented in further detail. Finally, in the research paper under the section entitled, Preventative Actions to Secure the E-mail System in the Healthcare Organization will include solutions to the aforementioned e-mail challenges the health care organization can implement, which represent the best practices for the security of the e-mail system, while enforcing HIPAA's and ECPA's legislative laws in the health care organization.

Keywords

Health Insurance Portability and Accountability Act (HIPAA), Protected Health Information (PHI), compliance, privacy, security, Business Associate Agreement (BAA), Electronic Communications Protection Act (ECPA), Electronic Protected Health Information (EPHI) and firewall, access control, and encryption.

Introduction

Since the implementation of the electronic medical record (EMR) in the health care organization, the security, confidentiality, integrity, and the availability of Electronic Protected Health Information (EPHI) has been the main concern for the health care organization. Not only are the former issues important concerns for the health care organization, but also the compliance of the Health Insurance Portability and Accountability Act (HIPAA) is of most importance. In relation to the HIPAA Security Rule, April 20, 2005 marked the deadline for the health care organization and other HIPAA defined entities to meet compliance regulations. (A Guide to the Administrative Safeguards of HIPAA's Security Rule, p.1). With the implementation of the EMR and the increasing number of electronic documents to safely and securely process, the health care organization began to utilize the fax machine and e-mail system for "…quick, secure, and reliable…" processing of the EPHI (Anonymous, 2001, p. 1).

For the purposes of the research paper, only the e-mail system will be the concern of the health care organization. Hence, understanding the uses of the e-mail system in the health care organization, the challenges of the e-mail system in the health care organization, and the preventative actions for securing the e-mail system in the health care organization will help the health care organization implement security's best practices by ensuring the security, confidentiality, integrity, and availability of the e-mail system in the health care organization, while protecting the privacy of the patient in the health care organization, thus, ensuring HIPAA compliance. HIPAA as well as The Electronic Communication Privacy Act (ECPA) play a vital role in EPHI. According to *American Online (2003),* The Electronic Communications Privacy act in the health care organization would constitute the following:

> The Electronic Communications [sic] Privacy Act (ECPA) sets out the provisions for access, use, disclosure, interception and privacy protections of electronic

> communications. The law was enacted in 1986 and covers various forms of wire and electronic communications. According to the U.S. Code, electronic communications "means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce." ECPA prohibits unlawful access and certain disclosures of communication contents. Additionally, the law prevents government entities from requiring disclosure of electronic communications from a provider without proper procedure. The Legal Institute provides Title 18 of the U.S. Code, which encompasses ECPA (American Online, 2003, p. 1).

Even more importantly, securely protecting the confidentiality and availability of the EPHI in the health care organization, while applying HIPAA and ECPA legislatures increases the integrity of the EMR, this should be the goal of the health care organization.

The Uses of the E-mail System in the Healthcare Organization

The health care organization uses the e-mail system for the daily processing of electronic documents. The health care organization process "…hundreds of documents daily in the course of providing patient care, collecting reimbursements, and responding to requests for health care information" (Anonymous, 2001, p. 1). Since many of these documents contain protected health information and are used to collect additional information, forward for signature or document other kinds of "…notification or receipt…" the security of the data is essential when electronically processing PHI in the health care organization (Anonymous, 2001, p.1). According to Crouch (2005), "…HIPAA applies to e-mail when confidential patient information is included in e-mail communications…: (p.1). With confidential patient information existing in e-mail correspondence, the health care organization faces many challenges on how to protect the sensitive data.

Challenges of the Healthcare Organization in Relation to HIPAA

The challenges of the health care organization in relation to HIPAA become a major concern when the external party or vendor receives e-mail correspondence. Even though there is an internal threat from the internal user, the HIPAA security deadline mandates the security and confidentiality of EPHI when being transferred from the health care organization to the external vendor or party. When dealing with the external vendor or party, the health care organization requires the external vendor or party to sign an Amend Business Associate Agreement (BAA).

The Amend Business Associate Agreement (BAA) is an important administrative safeguard that allows the health care organization to amend the HIPAA Security Rule to the business associate and any third party organization that accesses the EPHI. In addition, the BAA constitutes the requirement that the business associate places the necessary controls into effect to protect the confidentiality and integrity of the EPHI it accesses from the covered entity. Under the BAA, the business must report any HIPAA Security Rule violations immediately to the health care organization. The BAA also gives the health care organization the right to terminate the agreement when the business associate is guilty of violating the HIPAA Security Rule of the health care organization.

The external vendor or party the health care organization exchanges EPHI with may encompass the transcription vendor, lab vendor, doctor office, the hospital, the patient, the coder, and the regulatory agency for statistical information purposes. When the health care organization uses e-mail to transmit PHI, the health care organization faces the following challenges HIPAA compliance, verifying senders, "…ensuring privacy, combating spam and other e-mail threats…" (Crouch, 2005, p.1).

Remaining HIPAA compliant for the health care organization means adhering to the legislative laws in regards to the privacy and security of the PHI, as well as producing audit trails for every "…e-mail user…" when this information has to be presented as a part of the "… compliance audit…" (Crouch, 2005, p.1). Each health care organization should assess the individual risks for its organization. Every health care organization will not have the same risks in regard to HIPAA compliance, but it is very important for the health care organization to perform a risk assessment, risk analysis, and use risk management to help manage and remain HIPAA compliant, thus, eliminating the potential legal lawsuits from patients, and penalties and fines from HIPAA noncompliance. As well as the former, the health care organization can use an "…e-mail firewall as the last line of defense for a company, inspecting and applying complicated compliance-oriented policies to outgoing e-mail before the e-mail hits the public network" (*"Border Ware Technologies,"* 2005, p.2). Hitting the send button to transmit an e-mail with "… confidential and/or private information…" can constitute a HIPAA "…compliance violation (*"Border Ware Technologies,"* 2005, p.2). *Border Ware Technologies (2005)* also suggests that encryption as well as access controls may seem to be the obvious solutions to compliance, but since there is not a "…legal precedent to prove this former fact, the "…true lasting requirements…" are still incomprehensible.

The next challenge for the health care organization is the verification of the e-mail sender. With the rising numbers of Internet crimes, it is imperative the health care organization ensure the verification of an e-mail sender before PHI is routed back to the sender, only to compromise the patient's privacy and confidential patient information. Verifying the e-mail sender can be difficult sometimes, but the information can be detrimental to a patient if it falls into the "…wrong hands…" (Crouch, 2005, p.1). Crouch also states that implementing "…an encryption solution… with a '…digital signature on each encrypted e-mail…'" is one way the health care organization can verify the identity of the e-mail sender (p.1). Verifying the e-mail sender is also important to reduce the following risks of misuse according to Jurevic (1998), "The risks of misuse of this information are improper treatment, loss of employment, loss of insurance, loss of privacy, and reluctance to obtain medical care." (p.2).

Ensuring the privacy of communication is another challenge of the health care organization. According to an article entitled, *HIPAA Email Encryption and Security Compliance for Healthcare Professional (2005),*

> On April 14, 2003 [sic], the privacy protection provisions of the HIPAA legislation go into effect and pose a major compliance challenge for the The Health Care industry. The privacy provisions in HIPAA include:
>
> - protection against the unauthorized disclosure of a patient's "individually identifiable health information."
> - Each instance of unauthorized disclosure by a health care provider is punishable by fines ranging from $10,000 to $25,000.
> - Each instance of intentional unauthorized disclosure is punishable by fines ranging from $100,000 to $250,000 and possible jail time for those who violate the provisions.
>
> The HIPAA Security Standard contains two subparts that relate directly to data integrity, data access and mechanisms for handling data. These include:
>
> - **45 CFR Part 142, § 142.308 (c)**. "Technical security services to guard data integrity, confidentiality and availability." These are processes that protect information and control individual access to information.
> - **45 CFR Part 142, § 142.308 (d).** "Technical security mechanisms." These are controls that prevent unauthorized access to information that is transmitted across an internal network or across the public Internet (p. 1).

Each health care organization has to determine the best practices for securing the privacy of business e-mail communications and make sure it as easy as traditional e-mail without complicating the correspondence or exposing the health care organization to hefty HIPAA fines and penalties, thus, making secure e-mail communications user friendly. For non-technical users, the easy e-mail transmission of private PHI is an essential part of everyday business practices. Therefore, the health care organization must implement a solution, which ensures fast, easy, secure availability of the PHI. In other words, the e-mail end-to-end communication should remain private "…in transit and on the enterprise e-mail server" (Crouch, 2005, p.1). Ensuring end-to-end communication, would keep e-mail free from threats and enable the health care organization’s e-mail system to remain clandestine, private and acquiescent (Crouch, 2005). Not surprisingly, because each health care organization’s e-mail security safeguards concerning HIPAA may vary, the health care organization must again determine which technical and/or software solution (s) would best fit the needs of the health care organization’s e-mail system. In addition, the health care organization should continually manage these safeguards to eliminate the potential internal and external threats.

Finally, combating spam and other e-mail threats as well as mandates are of importance of the health care organization as well. The health care organization faces inbound threats as well as outbound threats/mandates (“*Advanced Email Security for Healthcare Organizations*,” webinar, p. 1). The inbound threats include spam, viruses, denial of service attacks, botnets, and phishing and directory harvest (“*Advanced Email Security for Healthcare Organizations*,” webinar, p.1). The outbound threats/mandates range from corporate governance, HIPAA (security, privacy, and compliance), and intellectual property (“*Advanced Email Security for Healthcare Organizations*,” webinar, p.1). The inbound and outbound threats travel through the Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP), and File Transfer Protocol (FTP) channels (“*Advanced Email Security for Healthcare Organizations*,” webinar, p. 1). Again, the health care organization should implement technical as well as software safeguards to eliminate the inbound and outbound threats/mandates in the health care organization. The preventative actions for securing the e-mail system will be discussed in detail in the next section of the research paper.

Preventative Actions to Secure the E-mail System in the Healthcare Organization

As formerly stated earlier in the research paper, when the health care organization uses e-mail to transmit PHI, the health care organization faces the following challenges HIPAA compliance, verifying senders, "…ensuring privacy, combating spam and other e-mail threats…" (Crouch, 2005, p.1). Therefore, when the health care organization implements a solution that secures the former challenges, the health care has started working toward a business solution for securing the e-mail system that is specific to its healthcare organization. There are various solutions available to the health care organization to help meet the challenges of the e-mail aforementioned formerly in the research paper.

Additionally, there are many HIPAA compliant solutions available for the health care organization. However, for the purposes of the research paper, the BorderWare MXtreme (MXtreme) will be discussed in more detail. The MXtreme can help the health care organization remain HIPAA compliance with the growing use of e-mail transmissions with PHI. "BorderWare MXtreme is an e-mail security and privacy and compliance solution that addresses key aspects of compliance requirements as they relate to e-mail" (Border Ware Technologies, p.5). MXtreme can examine, determine, deliver, and report on e-mail messages in relation to privacy and compliance within a health care organization (Border Ware Technologies, p.6). The examination step entails examining each message that passes through the gateway for sensitive and or private information (Border Ware Technologies, p.6). The determination step encompasses the solution's ability to determine what to do with an e-mail message upon the discovery of inappropriate content and the appropriate action to take on the inappropriate message (Border Ware Technologies, p.6). The next step is the delivery step, which addresses how to handle the inappropriate message based on the policies the health care organization has previously defined within the solution (Border Ware Technologies, p.6). For example, the following may be some defined policies "…allow, block, encrypt, copy to compliance officer, message stamping, return to sender, and audit/log" (Border Ware Technologies, p.6). The last step is reporting, which constitutes the solution's ability to document, record, and report on the messages to ensure the health care organization adherence to the compliance and regulations it has set up within the policies of the solution.

The use of e-mail encryption helps the health care organization to identify the sender of the e-mail, while protecting e-mails from hackers, who try to intercept and read them in transit. The application of encryption to an e-mail means the e-mail data is scrambled and only readable or un-encrypted by the use of the correct cryptographic key. The following are some of the popular e-mail encryption programs: Centurion Mail, Easy Email Encryption, Kerberos, HushMail, Pretty Good Privacy (PGP), Riordan's Internet Privacy, Enhanced Mail (RIPEM), Safe Message and Sure Hive. Encryption also ensures an end-to-end secure e-mail communications channel between the sender and the recipient of an e-mail. In other words, encryption ensures the privacy of the EPHI in the health care organization as well as identifies the sender of an e-mail.

One way to combat spam is to make sure the spam solution the health care organization implements is the best solution for the organization (*Advanced Email Security for Healthcare Organizations*," webinar, p. 6). Once the health care organization implements the solution, the e-mail administrator should continually measure the volume of spam in relation to percentage of effectiveness of the spam as it relates to how much spam is actually getting through the spam solution's filters (*Advanced Email Security for Healthcare Organizations*," webinar, p. 6). The health care organization should also try to better spam effectiveness to a 99 % level to help eliminate the amount of spam that gets through the spam solution and reduce the number of help desk calls in the health care organization (*Advanced Email Security for Healthcare Organizations*," webinar, p. 1).

Conclusion

The health care organization must realize that no e-mail solution is 100% risk free of inbound and outbound threats/mandates. The health care organization has the responsibility of continually updating, maintaining, and cost-effectively managing its e-mail solution. Realizing the fact that no software or technical solution can eliminate all potential threats or compromises faced in today's health care organization, the health care organization should stay abreast with vendor updates, changes to e-mail policies, updates on threats, performs risk identifications, risk assessments, and risk analysis. Understanding the uses of the e-mail system in the health care organization and the challenges of the e-mail system can help the health care organization determine the best e-mail solution for the organization. Once the health care organization identifies, configures, and implements, the e-mail solution on the health care organization's network, the e-mail administrator should continue to manage the solution to ensure adherence to security best practices. Moreover, ensuring the health care organization's security best practices help to maintain the security, confidentiality, and availability of the e-mail system in the health care organization, thus, ensuring the privacy and integrity of EPHI in relation to the HIPAA and ECPA laws and regulations.

References

Advanced Email Security for Healthcare Organizations. (n.d.)Retrieved on June 29, 2007 from, http://whitepapers.zdnet.com/webcast.aspx?cid=88&docid=291456&part=rss&tag=rss&subj=ZDNet&promo=100112

A Guide to the Administrative Safeguards of HIPAA's Security Rule. (n.d.). Retrieved July 15, 2006 from, http://www.utahbar.org/barjournal/archives/2006/04/a_guide_to_the_1.html

* Allman, Eric. Q focus: cybercrime: E-mail authentication: what, why, how? (Nov. 2006). *Queue*. Vol. 4, 30-34. http://delivery.acm.org.jproxy.lib.ecu.edu/10.1145/1190000/1180191/p30-allman.pdf?key1=1180191&key2=7534383811&coll=portal&dl=ACM&CFID=20657096&CFTOKEN=19998252

Anonymous. (2001). Secure messaging solutions for health care. Retrieved July 01, 2007 from, http://h71028.www7.hp.com/enterprise/downloads/healthcareBrochure.pdf

American Online. (2003). Electronic Communications Privacy Act. Retrieved on June July 01, 2007 from, http://legal.web.aol.com/resources/legislation/ecpa.html

Border Ware Technologies. (n.d.). When Pressing the “Send” Button Leads to Legal Liability. (November 2005). Retrieved on June 28, 2007 from, http://whitepapers.techrepublic.com.com/thankyou.aspx?authId=jq0MlVn6ofjwfmk+lFUexf2CWd/v988a1JcjeAE6g/H+mAEj4V4QYkLdNPcesp89&&docid=165939&view=165939&load=1

Crouch, Mary. Approaching HIPAA with E-mail Security. (2005, July 18). Retrieved on June 30, 2007 from, http://health-care-it.advanceweb.com/common/Editorial/PrintFriendly.aspx?CC=56709

*Francia III, Guillermo A. (May 2006). Digital forensics laboratory projects. *Journal of Computing Sciences in Colleges.* Vol. 21, 38-44. http://delivery.acm.org.jproxy.lib.ecu.edu/10.1145/1130000/1127360/p38-rancia.pdf?key1=1127360&key2=6273383811&coll=portal&dl=ACM&CFID=20657096CFTOKEN=19998252

HIPAA Email Encryption and security compliance for Healthcare Professional. Retrieved on June 15, 2007 from, http://www.authora.com/healthcare.asp

*Jurevic, Amy M. WHEN TECHNOLOGY AND HEALTH CARE COLLIDE: ISSUES WITH ELECTRONIC MEDICAL RECORDS AND ELECTRONIC MAIL. (Summer, 1998). Vol. 66, 1-1000. Copyright (c) 1998 University of Missour-Kansas City School of Law UMKC Law Review

Kopel, D. & Thompson, D. Government Eavesdropping via E-mail. (1999, July 4). *Dave Kopel.* Retrieved on March 17, 1007 from, http://www.davekopel.com/DigitEcon/OpEds/Government-Eavesdropping.htm

*Lynch, Jennifer. PART I: LAW AND TECHNOLOGY: II. CYBERLAW: A. NOTES: Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks. (2005). *Berkeley Technology Law Journal*. Vol. 20, 259. Copyright (c) 2005 Berkeley Technology Law Journal Berkeley Technology Law Journal

*Minsky, Naftaly H. Independent online monitoring of evolving system. (1996). *IEEE Computer Society*, International Conference on Software Engineering Proceedings of the 18th I nternational conference on Software engineering. 134-143. http://delivery.acm.org.jproxy.lib.ecu.edu/10.1145/230000/227753/p134-minsky.pdf?key1=227753&key2=3995711811&coll=portal&dl=ACM&CFID=20657096&CFTOKEN=19998252

*Spielberg, Alissa, R. Online Without a Net: Physician-Patient Communication by Electronic Mail. (1999). *American Journal of Law & Medicine.* Vol. 25, 267. Copyright (c) 1999 Boston University School of Law American Journal of Law & Medicine

The USA Patriot Act. (2005, November 17). Retrieved on March 17, 2007 from, http://www.epic.org/privacy/terrorism/usapatriot/

Whitman, Michael E., & Mattord, Herbert J. (2004). *Management of Information Security*. Course Technology: Boston, MA.