Global Information Assurance Certification Paper

HIPAA Regulations - Information Security and Health Care

David Methe _GSEC
October 23, 2002
Version 1.4b

Abstract

The Health Care industry, has long wrestled with the challenges of maintaining the security and confidentiality of patient health information. In 1996, Congress established the Health Insurance Portability and Accountability Act, referred to as HIPAA, one component of which is to ensure the security of electronic health care data. In addition to regulatory compliance requirements, health care organizations and facilities face the same security challenges as any entity conducting business in the information age.

The intention of this study is to discuss the unique challenges faced by health care organizations with respect to information security by highlighting various security vulnerabilities. The study discusses how information technology controls can be applied in a health care environment to protect personal health information to achieve compliance with the HIPAA Security regulations.

This study begins by presenting a brief overview of the HIPAA regulations. Various examples of data security and privacy vulnerabilities are presented. The study then focuses on a vulnerability cited within the hypothetical example; the risk associated with the unauthorized installation of software on user desktops, with particular emphasis on the currently popular Instant Messaging application or “Chat”.

Introduction

Advances in technology and the proliferation of data warehousing and mining, particularly in the healthcare industry, have posed increasingly greater challenges for IT and Security professionals to ensure the protection of the data. The implementation and use of security tools and mechanisms has lagged behind the upsurge in the development and use of new information systems.

In recent years, the health care “consumer” (i.e. patient and/or insured) has demanded that the industry take steps to protect their privacy, by limiting how and to whom their personal health and demographic

information can be shared among the various constituents in the health care industry. Congress responded with the Health Information Accountability and Portability Act (HIPAA). The scope of the legislation is broad. One of the main objectives of HIPAA is to ensure continued health care coverage for employees as they transition from one employer to another (i.e. portability). Administrative simplification is another objective of HIPAA, which establishes EDI standards for various health care transactions. Lastly, HIPAA includes requirements on the health care industry to protect the privacy and security of individually identifiable health information. The privacy side of the legislation deals with the conditions under which "covered entities" (e.g. hospitals, doctors, labs and health insurance companies) and their employees are authorized to posses and share "protected health information" (PHI).

The Security aspect of the legislation, which is the main focus of this presentation, pertains to "how" health information is protected. In particular, the legislation consists of four major components to safeguard the integrity, confidentiality and availability of data:

- **Administrative procedures.** These include policy, procedure and the conduct of personnel in relation to the protection of data, including password use policies, incident reporting procedures, and termination procedures.
- **Physical safeguards**. These relate to the protection of physical computer systems and related buildings and equipment (e.g. from fire or sabotage). Physical safeguards also cover the use of locks and keys to control access to computer systems, workstation location and use, and disaster recovery plans.
- **Technical security services.** These include the processes that are put in place to protect, control and monitor information access. Examples include audit controls and authorization controls such as unique user identification and auto logoff features.
- **Technical security mechanisms**. These are focused on preventing unauthorized access to data that is transmitted over an "open communications network". In essence, this part of the regulation requires the use of encryption when sending PHI over the Internet.

The Rationale for Health Care Security Regulations - Identifying Security Gaps

To illustrate how broad the scope of information security can be, let's take a simple hypothetical example: Mrs. Smith visits her general practitioner because of a sore throat, is referred to a specialist, and ultimately is admitted to the hospital for surgery to remove her tonsils. Let's assume that Mrs. Smith is a member of an HMO whose premiums are paid in part by her employer.

Now let's consider some of the instances where Mrs. Smith's personal health information could be compromised within this example. The following items consist of a specific scenario related to Mrs. Smith's treatment, and an associated risk of unauthorized or unintended disclosure of information.

1) **Scenario**: The day before Mrs. Smith's office visit, a staff member from the Dr.'s office logged into the HMO's web site to verify Mrs. Smith's eligibility and health coverage.

   Vulnerability: The HMO maintains a web site, which contains PHI. Under the HIPAA requirements for Access Controls, the HMO must ensure that minimum necessary access is granted to health care workers. Authorization to access PHI must be either user-based or role-based. Employees must use a unique login IDs and password to access PHI, and login accounts may not be shared among health care employees [1]. The HMO then is faced with a unique security challenge in this scenario. When using the Internet to share patient information with other entities, how does the HMO ensure compliance with HIPAA regulations? Does the HMO have the ability to audit and sanction the behavior of the physician's office staff?

2) **Scenario**: While Mrs. Smith was in the doctor's crowded waiting room, the receptionist called out her name once the Dr. was ready to see her.

   Vulnerability: HIPAA law regarding "minimum necessary" access requires that covered entities make reasonable efforts to limit access to PHI. In some cases, it may be necessary for a doctor's office to modify their practices, and perhaps even remodel their waiting rooms to better accommodate the confidentiality of patient information. One example is for the doctor's office to use paging devices similar to what restaurants use, as a way to call patients in from the waiting room.

3) **Scenario**: When she was referred for more tests, the Ear, Nose and Throat specialist asked for a copy of her full medical history, which included information about her hysterectomy.

   Vulnerability: The HIPAA regulations require that covered entities apply "minimum necessary " standards when deciding who may have access to personal health information. In this case, it is acceptable for a specialist directly involved the patient's care to have access to the full medical history. However, hospitals and HMOs are constantly

faced with similar, but often less certain scenarios regarding the sharing of PHI.

4) **Scenario**: When Mrs. Smith was admitted to the hospital for surgery, the hospital received a telephone inquiry about her condition from an out-of-state family member.

   Vulnerability: Well meaning hospital employees have been known to disseminate patient health information inappropriately. Furthermore, employees are susceptible to "social engineering" attacks [2], and should receive awareness training to mitigate the risk of such attacks. As a result of the HIPAA legislation, hospitals (and all covered entities) must conduct security training, and are also required to institute specific policies governing the dissemination of PHI.

5) **Scenario:** Mrs. Smith's surgeon discusses her procedure with a colleague while waiting in the lunch line in the hospital cafeteria.

   Vulnerability: This is another example of how data confidentiality may be compromised by well meaning but untrained employees. HIPAA guidelines require that covered entities conduct regular security awareness training for all health care employees.

6) **Scenario**: While updating Mrs. Smith's electronic chart in the recovery unit at the hospital, the floor nurse momentarily steps away from his workstation to tend to an urgent issue.

   Vulnerability: Physical security and workstation proximity are addressed in the HIPAA regulations. In this example, the nurse logged into the workstation (presumably with his own unique user ID), and left the workstation exposed to the possibility that someone else with less security clearance could access Mrs. Smith's medical data.

7) **Scenario**: In order to provide outcome measures and cost performance ratios to the doctors, the HMO developed an ad-hoc reporting system and places it on a secure web server that the doctors can log into and view information on their particular patient panel.

   Vulnerability: When using the Internet as the media for which to present PHI, it is incumbent on the HMO to have appropriate perimeter protections to secure the web server. HIPAA also requires the HMO to have intrusion detection mechanism in place [3].

8) **Scenario**: In response to the employer's request to justify a rate increase, the HMO created a report, which indicates that they received and paid claims for 23 employees during the 1st quarter of the year. The report was written to a CD and mailed to the employer. Although the report omitted employee names, it includes information such as date of service, treatment, and cost. (The employer is aware of which employees were out on personal leave during that time, and could likely determine that it is indeed Mrs. Smith who was the single highest user of employee health care benefits in the company).

   Vulnerability: The HIPAA regulations require that each covered entity have a signed "Business Associate Agreement" with every business partner with which personal health information is shared. The agreement limits what the business partner can use the information for. Further, information that is shared in this way must be "de-identified" such that someone could not derive the identity of a patient based on supporting data. Another potential risk to be noted in this example is the lack of guidelines for the handling of the CD. Did the HMO require the employer to return or destroy the CD once the reporting need was fulfilled? If not, the CD could end up being pulled out of trash bin by someone and posted on the Internet.

9) **Scenario**: To facilitate an outsourcing arrangement the HMO has with another company, a VPN tunnel was implemented to allow contract employees to remotely access the database and process claims on behalf of the HMO.

   Vulnerability: Implementing a virtual private network introduces a degree of risk to network security. Whereas many of the preceding examples dealt with risks to data *confidentiality*, this example demonstrates a risk to data *integrity*, and potentially data *availability* if the VPN security is compromised. Therefore, it is necessary for the HMO's Information Security Officer to assess the threats and vulnerabilities associated with the VPN configuration, in order to evaluate and control the security risks (risk = threat x vulnerability).

10) **Scenario**: Some employees of the HMO and the physician's office installed IM (Instant Messenger), AKA Chat software on their desktops in order to communicate directly about member eligibility, referrals and claims status.

Vulnerability: Although installing IM software was done to meet a specific business need, the software was not sanctioned by the employee's respective Security Officers, and was installed without the knowledge or consent of the employers. The risk associated with this scenario is high due to the fact that end-users, who may be ignorant of the risks, may be inclined to install software on their PCs without proper authority, if they perceive it to be useful.

The above list represents just a small sample of the ways in which PHI can be compromised. In the absence of proper security safeguards and procedures, Mrs. Smith's personal health information will almost certainly be exposed to unauthorized persons due to incidental, unintended disclosure alone. When the prospect of malicious intent (i.e. hacking) is taken into consideration, the likelihood of an unauthorized disclosure is even greater. It is easy to understand then, the demand for security legislation in the health care industry. In the next section, we will focus our discussion on scenario number 10, and highlight some of the specific network security risks associated with corporate use of the IRC protocol.

IM and Workstation Security Threats

According to a recent survey performed by Osterman Reseach, "IM is being used, either officially or unofficially, in 84% of the organizations surveyed." Furthermore, they report that that figure is expected to continue grow significantly in the future [4]. However, most IT departments have not implemented any firewall blocking related to IRC, either because a management decision has been made to use the tool without a proper risk assessment, or it is being installed and used in the organization without management's knowledge and consent.

Using IM without proper policies and security safeguards in place can and expose a network to a number of security risks. In general, firewalls operate on the premise that if the IP traffic originated on the inside of the network, then it is OK to let the return traffic into the network. IM clients have evolved over time to circumvent corporate firewall filters by tunneling known ports.

Buffer overflow vulnerabilities have been consistently reported in MSN Chat and Microsoft Instant Messenger software, as early as Chat version 2.0 for Windows 95 [5]. Buffer overflows allow an attacker to run malicious code on a system that contains the vulnerability, thereby taking full control of the device. A hacker can further exploit a buffer overflow by running code, which modifies the host's security settings, thus introducing new vulnerabilities to be taken advantage of at a later time. An attacker could

also use the buffer overflow to plant code to help launch a DDOS attack on other systems. A recent example of a buffer overflow vulnerability is the MSN Messenger MCX, which exists on un-patched versions of Instant Messenger 4.5 and 4.6 [6].

Hackers may also use IM as a vehicle to conduct social engineering attacks. Most recently, a worm called "Henpeck" was spreading via MSN Messenger by convincing users to download a file. Once executed, the file propagates by resending itself to members of the user's buddy list [7].

But the risks of using IM go beyond technical security exposures. They also include vulnerabilities to data confidentiality, even when appropriate technical controls are in place. As an example, employees may believe they are complying with their corporate security policy by not sending confidential information via email, but then transmit sensitive across the Internet in a chat session. Encryption of data and strong authentication of remote users is beyond the means of the average end user to perform. They may also be unaware that most IM applications are not truly peer-to-peer, but utilize a central server that logs and relays the messages. Which means that the chat text is logged on a server somewhere, and could potentially be read, copied or redistributed by a hacker. Perhaps the most notable example of a compromise of data security resulting from the corporate use of IM is that of Efront Media, Inc, when the a company who's CEO and other top executive's confidential IM communications were made public by being posted on the Web [8].

Safeguards to Mitigate IM Risks

Policy:

As a general rule, corporate security policies should prescribe that unneeded system features, functionality and services be disabled. Adopting this philosophy will assist an Information Security Officer in the challenge of fully comprehending security risks introduced by a new technology, before the end-user community hears about it and decides to use it. However, adopting a security philosophy, and enforcing a security policy at the desktop level are two different things.

Workstation Level:

In a Windows 9x environment, Security Officers and IT Departments had to rely mostly on policy to prevent user-installed software. If an organization did not exercise appropriate sanctions for policy infractions, then the risk could not be easily controlled. Since the advent of Windows XP, administrators can leverage OS features like Microsoft Baseline Security Analyzer to assist with patch management, and Software

Restriction Policies [9] to deny unauthorized downloading and installation of software.

There is a host of third-party tools available for both Unix and Windows environments to assist administrators with the task of hardening workstation security. Shavlik has a suite of tools, which includes "Personal Security Advisor". PSA scans for security vulnerabilities and provides patch management reports for all current Windows versions, and MS desktop products including Office and Outlook. [10].

Perimeter Level:
Network Analysts can attempt to contain the unauthorized use of IM by locking down ephemeral firewall ports. However, some IM applications have begun to circumvent firewall filters by designing their products to use common ports like port 80. This makes IM difficult to track, and even more difficult to stop at the firewall without impacting employee's ability to browse the Internet.

A variation of the DOS attack against IM clients is the ICMP bomb. This is carried out by flooding a device with forged ICMP messages such as ?host unreachable packets, with the intention of terminating the active connections between the victim and the device it was communicating with [11]. According to the CERT Coordination Center: "To prevent denial of service attacks based on ICMP bombs, filter ICMP redirect and ICMP destination unreachable packets. In addition, sites should filter source routed packets." [12]

Conclusion

In the final analysis, IM is more of a toy for home use than it is a productivity tool for business, particularly a health care business.

The HIPAA regulations are "technology neutral", so they are void of any specific recommendations about products, vendors, policies or procedures. It is up to the Information Security Officer in each health care organization to consider the benefits that a technology will yield, against the risks it contains. Consider though that EDS, and multinational consulting company with over 140,000 employees recently banned the use of IM corporate-wide [13]. Although a drastic measure, decision makers at EDS obviously recognized that the risks associated with IM outweighed the benefits.

When it comes to protecting your business' most important asset, the only totally secure measure is to limit your tool-set to those that can be hardened, managed and tracked. In my opinion, if there is not a

preexisting business justification for using IM, then the decision is easy. Take a lead from EDS, and avoid a multitude of potential security risks altogether.

References

1. Britton, Alexander; Pashkoff, Dana; Tedesco, John – The HIPAA Handbook: What Your Organization Should Know About the Proposed Federal Security Standards". Washington, DC: URAC/American Accreditation HealthCare Commission, 2002, 62-63.

2. Sarah Granger, - **"**Social Engineering Fundamentals, Part I: Hacker Tactics"
   URL: http://online.securityfocus.com/infocus/1527

3. Phoenix Health Systems, HIPAAdvisory - "Intrusion Detection"
   URL: http://www.hipaadvisory.com/tech/IntrusionDetection.htm

4. Osterman Research, Inc. - "Survey on Instant Messaging"
   URL: http://www.ostermanresearch.com/results/surveyresults_im0902.htm

5. Microsoft, Inc. - "Microsoft Knowledge Base Article - Q321661"
   URL: http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q321661&

6. eEye Digital Security – "MSN Messenger OCX Buffer Overflow"
   URL:
   http://www.eeye.com/html/Research/Advisories/AD20020508.html

7. Lemos, Robert, CNET – "Henpeck Worm Cons MSN Chat Crowd", October 10, 2002,
   URL: http://news.com.com/2100-1001-961693.html

8. Festa, Paul, CNET – "ICQ logs spark corporate nightmare", March 15, 2001, 11:05 AM PT
   URL: http://news.com.com/2100-1023-254173.html?legacy=cnet

9. Microsoft, Inc. – "Software Restriction Policies"
   URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/prdd_sec_ghxn.asp

10. Shavlik Technologoes, Inc. – “Shavlik Personal Security Advisor”
URL: http://www.shavlik.com/security/

11. Engarde Systems, Inc. – “Example Vulnerabilities”
URL: http://www.engarde.com/consulting/pentest/vulns.php

12. CERT – “Packet Filtering for Firewall Systems”
URL: http://www.cert.org/tech_tips/packet_filtering.html

13. The Register – “EDS bans IM”
URL: http://www.theregister.co.uk/content/archive/25185.html