GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Appropriate: A Small Business Search for HIPAA Compliant E-mail Security

R. Dayle Alsbury
12 April 2004
GSEC Practical Version 1.4b
Option 2

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

The health care industry has come to rely so heavily on the medium of electronic communication that the United States Federal Government has enacted legislation to regulate how private health information is handled, including the transmission of e-mail. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted to regulate the availability, confidentiality, integrity and usage of patient electronic protected health information. This regulation has had a direct and significant impact on the e-mail transmission of electronic protected health information.

This paper will focus on one small health insurance business efforts to comply with the e-mail transmission privacy and security requirements of HIPAA. This paper will present the case of how and why a small business determined that it had reached the size where it could reasonably address its growing HIPAA e-mail compliance issue. The paper will also show how its solution met the compliance standards of the HIPAA security regulations. Finally, this paper will discuss the positive and negative technical components of its choice of HIPPA compliant e-mail solution.

I. The Problem Identification; a Snapshot before Resolution:

I. A. Situation Overview

This case study is of a small insurance business providing both health and non-health related products which are separated by divisions. HIPAA regulations impact approximately half of the user base in the business. The e-mail communications system is not segregated by divisions. Desktop e-mail clients are separated into two distinctly HIPAA and non-HIPAA divisions.

The business is comprised of a <100 member e-mail user base. Approximately half the users transmit Electronic Protected Health Information (EPHI). This number is increasing as the health sector of the business expands.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Business expansion has resulted in more users transmitting EPHI via e-mail. There are now approximately 36 users transmitting approximately 5000 unsecured EPHI messages via e-mail, per year. Only large patient billing files had any sort of security during e-mail transmission. Verification of benefits, claims information and enrollment information are the EPHI that have most commonly been transmitted in-the-clear (i.e. unsecured).

The concept of in-the-clear communication transmission is similar to the postal mailing of a post card. Both the sending party and the receiving party can view the sent message, as well as anyone else that intercepts it. Reading an intercepted e-mail message is almost as easy as reading the intercepted post card.

Transmission security consisted of using encrypted compression ('zipping') with password protection on large patient billing files. The users were zipping the files because recipient systems would frequently filter the e-mail if the file was transmitted with the source spreadsheet. Additionally, users were utilizing a single, easily inferable word as a file password for all recipients.

Several users would request delivery receipts when transmitting files; however not all e-mail systems would respond with the requested delivery receipt. Consequently, some of the users would follow-up with long distance telephone calls (which increases operating costs) while others would assume the e-mail was delivered (and wait for further communication from the intended recipient if the file was not delivered).

Managerial inclusion and oversight was practically non-existent. There was no mechanism in place for management to independently control or audit internal or external user e-mail security practices. Management relied on the users to decide when and how to secure EPHI messages. In a nutshell, there were no access controls, integrity checks, authentication validation nor auditing control processes in place.

I. B. The Legal Environment:

HIPAA is a set of sweeping federal regulations that requires health care organizations and businesses that handle confidential patient health information to simplify and standardize data exchange in an effort to protect the security, privacy and confidentiality of that information. HIPAA established a set of uniform standards for the privacy of patient health information used by health plans, hospitals, pharmacies and other covered entities. These regulations cover the electronic, oral and printed data exchange of individually identifiable health information. The HIPAA regulations are administered by the Department of Health and Human Services (DHHS).

The core of the administrative and functional HIPAA requirements is established in the security and privacy standards of the HIPAA regulations. The HIPAA privacy standards section of US 45 CFR 164.530(c)(1) is the regulatory section that delineates standards of how healthcare organizations will protect individually identifiable health information. The standards, known as The Privacy Rule, spell out these administrative safeguards standards. This section's

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

safeguard standards establish that "a covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information".

The key word in the rule is "appropriate", because it's left up to the covered entity to define appropriateness for itself, within reason. Neither HIPAA nor the US DHHS define appropriateness because there is no one size fits all measure. The appropriateness of any safeguard standard is viewed as relative to the size, nature, and capacity of each business. Therefore, adherence to The Privacy Rule safeguard standards is relative.

We also focused on the Technical Safeguards section of the HIPAA security standards established in US 45 CFR 164.312. The standards, also referred to as the Security Rule, established five security standards for electronic protected health information (EPHI) protection; access control (unique user identification, emergency access, automatic logoff, and encryption), audit controls, integrity, authentication, and transmission security.

The Technical Safeguards section of the regulation defines both "required" and "addressable" safeguard standards. The required standards must be implemented according to the specifications established in the regulation. The standards that are listed as addressable may be implemented in whole, implemented in combination with an alternative specification or implemented by alternative specification. The regulation further requires the organization to document its decision, rationale, and elected approach if an alternate specification is implemented.

I. C. The Legal Risk:

HIPAA regulations are backed up by stiff civil and criminal penalties for non-compliance. HIPAA was the first federal law to impose criminal penalties for the improper use and/or disclosure of protected health information. HIPAA imposed penalties can range from "$100 per violation, up to $25,000 per year for each requirement violated". (Weil 2). Criminal violations can result in civil and penal penalties "from $50,000 in fines and one year in prison up to $250,000 in fines and 10 years in jail". (Weil 2)

The most potentially damaging possibility of a HIPAA privacy breach is the loss of business, negative public impact and possible civil suit damages that such a disclosure would bring. The potential damage from a HIPAA violation could far exceed the federally mandated penalties.

I. D. The Technical Risk:

The legal risk was simply a reflection of the underlying technical risk. The fact that we were transmitting e-mail messages without any encryption or policy based filtering meant that we were transmitting unsecured PHI.

Intercepting e-mail transmissions is not a difficult task. A mail message bound for an external client may cross 3, 5, 10 or more Internet Service Providers (ISPs) or mail relay systems before it reaches its final destination.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Anyone with administrative access at any of these relay points could intercept and then view, edit, or copy the message prior to final delivery. Thankfully, the vast majority of ISP administrators do not intercept e-mail messages. The more nefarious scenario is that of the computer hacker.

Computer hackers can also intercept electronic transmissions. Hackers commonly employ a tool called a packet sniffer, which can monitor and intercept data on almost any TCP based network. A hacker could configure a packet sniffer to silently intercept information as it traverses one of theses relay points, the destination network or any unsecured device involved with the transmission.

Although e-mail interception and packet sniffing are not something that most administrators encourage or allow, it does happen. Because it does happen, we should understand that transmitting unsecured e-mail messages is inherently trusting in the kindness and security effectiveness of strangers.

II. The Problem Definition, a Snapshot during Resolution:

II. A. The Vulnerability Review:

What do we do to protect e-mail from being intercepted and viewed/modified/deleted? We encrypt it. E-mail encryption is a mathematical exercise that hides information in plain sight. Encryption applies mathematical formula manipulation to the e-mail message (including attachments) so that the message contents are hidden from anyone except the recipient key holder.

By not using message encryption we were sacrificing control of our EPHI. Once the message left our system, we had no real control over what happened to it. Our lack of EPHI encryption problem was:

1. Messages were being transmitted in the clear. Each message was wide open to exploitation if it was intercepted or sent to the wrong party.
2. Management lacked the ability to end-to-end audit message security & authenticity.
3. Messages lacked non-repudiation. We couldn't prove who sent and received messages transmitted from our system.

II.B. Vulnerability Awareness:

So how did this situation gain attention? It starts with a seemingly unrelated issue; zipped files.

The W32.Bagle worm was launched during March of 2004. The worm attempted to deliver its malicious payload by using zipped file attachments. The worm would hide itself inside of a zipped file attachment that would bypass most anti-virus filters. Once delivered, the worm would open a backdoor that allowed a "remote attacker to penetrate the victim's machine" (Symantec 1). The worm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

programmer apparently chose to use zipped files to transmit the payload because most anti-virus and anti-spam filters were not screening these files by default. The end result of the W32.Bagle worm was that most of the anti-virus scanners employed by the customer base began actively screening zipped files.

Shortly after the new filters became available, I received a call from some of our internal users requesting assistance with an e-mail problem. The initial complaint was that several of our customers could not receive e-mail from our e-mail server domain. Further investigation revealed that internal users were transmitting zipped files, via e-mail, to those customers. The e-mailed zipped files were being screened and dropped by the external user's anti-virus defenses. Initially this seemed like a minor configuration issue until I discovered that the information within the zipped files was replete with patient claims and billing information that met the definition of "protected health information" from 45 CFR 160.103. The revelation that our internal e-mail users were utilizing these zipped files to transmit EPHI changed the entire landscape of acceptable solutions for this problem.

The investigation of this issue revealed the following:

1. 5 users were transmitting large volumes of EPHI in zipped format on a daily basis.
2. 15 users were transmitting 5+ EPHI type messages in-the-clear on a daily basis.
3. 15 users were transmitting 2+ EPHI type messages in-the-clear on a weekly basis.
4. An initial estimate of 1 EPHI e-mail, per user, per day yields almost 5,000 non-HIPAA compliant (in-the-clear) EPHI e-mails per year.

Three end-user misperceptions were commonly voiced during the investigation;

1. Any zipped and/or password protected file qualified as HIPAA compliant EPHI security.
2. Delivery receipts were non-repudiating proof that the correct party had received the transmitted message.
3. Delivery receipts guaranteed message integrity.

II. C. Identification of Needs:

My first step was to determine if the HIPAA regulations applied to this company. I struggled with how to define of what constituted an appropriate measure when considering how to address the HIPAA Privacy Rule. I searched through HIPAA specific legal opinion on the topic. HIPAA-Attorneys.com archives advise that when "determining which specific technologies and security measures must be taken in order to meet the standards, an organization is permitted to take into account: its size, complexity, and capabilities; the costs of security measures; and the probability and criticality of potential risks to electronic protected health information" (Wachler 5). The physical and fiscal size of our organization, the volume of EPHI related e-mail and the wealth of information gained from the SANS Network Security Conference, November

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2003 (New Orleans) indicated to me that a fully functional HIPAA compliant e-mail security solution was now appropriate for this company.

After some discussion with upper management, it was determined that we needed to either develop or locate a HIPAA compliant e-mail security solution. Since we are a small company with limited Information Technology resources, we quickly came to the conclusion that we did not have the personnel time to develop our own solution. So, we decided to begin reviewing the commercially available options.

My second step was to identify the required technical safeguards of the HIPAA Security Rule. HIPAA section 164.312 separates the technical safeguards into required and addressable items and, when necessary, establishes implementation specifications.

HIPAA Technical Safeguards:

1. Required Technical Safeguards:
    a. Access Control – The system may only allow access to authorized persons.
        i. Unique user identification is required for each person.
        ii. Enable access to EPHI for emergency situations.
    b. Audit Control – The system must provide a mechanism for auditing EPHI usage.
    c. Authentication – The system must authenticate user access to EPHI.
2. Addressable Technical Safeguards:
    a. Access Control - Only allow access to approved persons.
        i. An inactive user must be automatically logged off.
        ii. EPHI must be electronically encrypted.
    b. Integrity – The system protects EPHI from unauthorized modification or destruction.
    c. Transmission Security – Protect EPHI communication.
        i. Integrity controls ensures that the EPHI was not modified or destroyed during transmission.
        ii. EPHI is encrypted during message transmission.

My third step was to identify the similarities between the end-user and managerial requirements for any proposed solution. Follow-up end-users interviews revealed they had the following requirements (**User Requirements**):

1. Message security (The message must only be reviewable by the destined recipient.)
2. Message integrity (The message transmission must not be compromised.)
3. Ease of use (It must be easily explainable and trainable to both the internal and external users.)
4. Delivery receipt (The end users required a non-reputable receipt as a proof of message reception.)

The management requirement list, although similar, was more detailed for technical and legal reasons. The list of management requirements for a HIPAA compliant e-mail solution was broken down into two categories; technical &

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

administrative (**Managerial Requirements**):

1. Administrative:
    a. Budget conscious ('appropriate' is measured by cost)
    b. Scaleable on a single user basis
    c. Easily trainable (must be easily trainable to internal and external uses)
    d. External user secure reply (external users must have the ability to securely reply)
    e. Delivery receipt archive
2. Technical
    a. Message Integrity (guarantees that the message was not altered)
    b. Non-repudiation (able to satisfactorily prove message authorship)
    c. Strong encryption (128 bit or higher)
    d. Universally available (must work on the majority of commonly available mail platforms)
    e. Minimal support (minimize routine technical support)

II. D. Solution Evaluation & Implementation:

For the review, I looked at the administrative, technical and physical safeguards available to the company. The consensus determination of the review was that our business size, PHI volume, transmission frequency, and requisite technical staff training had reached the level where a proactive solution seemed appropriate, technically feasible and fiscally viable.

The three factors that constrained the solution constraints were compliance, funding, and time. The proposed solution must be HIPAA complaint, fit within our budget, and it must be implemented within six weeks. Since I was dealing with a compressed time frame, I focused on those solutions that were explicitly presented as HIPAA compliant. Since I concentrated on explicitly compliant solutions, I will reserve a discussion of how compliance was achieved for the proposed solution, only.

As I began collecting literature on the subject it became obvious that potential solutions could be grouped into three distinct categories; server based, desktop based and subscription based.

II. E. Policy Server Options

I began by investigating locally installed and managed server based solutions. I began by conducting a brief review of the feasibility of employing a solution known as Pretty Good Privacy (PGP). PGP is a widely recognized and respected encryption technology. However, the limitation of our internal PGP expertise and funding seemed to preclude serious consideration of the PGP server based solution. A review of my personal conference notes from the SANS Network Security Conference, November 2003 (New Orleans), revealed a detailed discussion of the difficulties of creating a PGP server solution. The

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

conference notes confirmed our initial evaluation that creating a PGP server solution would be more costly and time consuming than we could afford.

The server based solutions were generally a mixture of locally managed servers that filtered all inbound and outbound e-mail transmissions through a set of policy criteria in an effort to filter and securely transmit (i.e.: 128 bit or stronger encryption) HIPAA related messages. The policy criteria are developed and maintained by the local Information Systems staff. The policy server based solutions run on a locally installed server that requires an initial expenditure typically starting in the thousands of dollars. Many of the policy server based solutions require a significant (in relation to our budget) annual maintenance contract/subscription as well as continual manual refinement of the policy criteria.

I measured the pros and cons of the policy server approach in relation to how they met the User and Management Requirements.

1. Pros:
    a. Met User Requirements 1 - 3
    b. Met Managerial Requirements 1b, c, e 2a, b, c & d
2. Cons:
    a. Some failed to meet User Requirement 4
    b. Failed to meet Managerial Requirement 1a & d and 2e

The costs, setup and support time were the most significant negative factors that eliminated a policy server based solution. I reviewed several policy server based solutions, but refrain from giving a detailed analysis of their inner workings as that is not the focus of this paper. I felt drawing attention to the unselected products could possibly prejudice the reader's perception of those products.

II. F. Desktop Options

After the server based options proved to be beyond our means, the pendulum swung in the other direction and I began looking for solutions at the desktop level. Desktop solutions met the first two criteria because they fit reasonably within our budget and implementation time frame. The desktop solutions I reviewed were desktop applications that interfaced with the business class e-mail clients from Microsoft, Novell, and Lotus.

These solutions are designed to either automatically or manually convert e-mail transmissions into HIPAA compliant encrypted messages, at the desktop. Typical setups involve user interaction (i.e.: clicking a button) to encrypt a message. These solutions typically used a single private-key encryption model where the key and encrypted messages are sent from the encrypting desktop to the external recipient. There is no management awareness of what, when or to whom the encrypted message was transmitted.

These solutions normally do not necessarily require annual subscriptions. The installation is handled by local Information Services staff and maintenance is minimal, usually only involving application updates or fixes.

There were several negative aspects of these desktop solutions. The lack of management awareness of the transmission traffic was significant because it

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

eliminated the possibility of management oversight. Additionally, since the application was tied to the desktop mail client, the application was susceptible to unauthorized use and therefore weak on non-repudiation. Another significant negative factor was the lack of secure reply feature available to the external recipient. All recipient replies would be in-the-clear.

I measured the pros and cons of the desktop encryption approach. The pros and cons for our situation were:

1. Pros:
    a. Met User Requirements 2 - 4
    b. Met Managerial Requirements 1a - c, 1e, 2a, c - e
2. Cons:
    a. Failed to meet User Requirement 1
    b. Failed to meet Managerial Requirements 1d & 2b

The lack of desktop security as it relates to non-repudiation was a significant negative factor. When combined with the lack of available management oversight, the non-repudiation weakness eliminated further consideration of a desktop based solution. I have listed the desktop solutions in the bibliography.

II. G. ASP Service Options

The final secure transmission model I investigated was based upon a subscription based service. This model utilizes a 3rd party hosted mail client for secure delivery. Typically, the Application Service Provider (ASP) will engage delivery by interfacing either a desktop or server based application in the initiating network. The message is secured and delivered to the ASP hosted mail server while a notification message is forwarded to the intended recipient. The intended recipient then actively requests delivery of the message at the secured ASP hosted mail site. To the recipient, this appears very similar to the mail method used by Microsoft, Hotmail and Yahoo.

The ASP subscription model is a 3rd party managed approach that satisfied two of our constraining criteria; cost control and rapid deployment. Because it's single or small block scaleable, this solution is able to provide a controlled cost per active user. Typically, these solutions cost a fraction of the typical policy based server and very close to the unit cost of the desktop model. Rollout time is typically faster than the policy server based solution, and about the same as desktop options. Additionally, this approach has near universal support across external user platforms, thus providing a secure reply method.

These solutions surrender a slight advantage to policy based servers in encryption integrity and non-repudiation because the message resides on a 3rd party mail server until the recipient takes delivery. The two most significant shortcomings are continual account support and lack of management control. The ASP model requires more interpersonal communication between the internal senders and external recipients due to the misunderstandings that can arise with the participants when using a 3rd party site (i.e. account passwords, first time use, etc.). Management's inability to forcibly encrypt all inbound and outbound

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

messages means that the responsibility for message encryption lies with the internal users.

I measured the pros and cons of the subscription based approach. The pros and cons for our situation were:

1. Pros:
    a. Met User Requirements 1 - 4
    b. Met Managerial Requirements 1.a, c-e, 2a-d
2. Cons:
    a. Failed Managerial Requirements 1b & 2e

III. The Solution, a Snapshot after Resolution:

The technical and administrative analysis clearly showed that the subscription based model met the most solution criteria. In a nutshell, the subscription model gave us the biggest 'bang for the buck'. Product reviews and interviews with industry peers led us to interview an ASP based subscription service offered by Certified Mail. Initial response from management and end users was positive so I proceeded with a technical investigation of this opportunity.

First, I will give an overview of the Certified Mail model followed by an explanation of how it satisfied some User and Management requirements and failed to satisfy others. Next, I will demonstrate how the chosen solution met & exceeded the technical standards of the HIPAA Security Rule. Finally, I will follow with an explanation of how & why Management chose this model in light of its benefits and draw-backs. .

III. A Solution Overview

The Certified Mail (CM) ASP model uses a combination of desktop application, secured servers and transaction confirmation to provide message integrity, security and non-repudiation.

CM starts by providing an application payload that interfaces with the desktop mail client (in our case, Microsoft Outlook 2002 and 2003). The application is registered with the end user's e-mail address during installation as part of the registration and security setup. A secondary Send button is installed onto the local mail client toolbar. The internal e-mail user composes the e-mail message (with or without attachments) as normal, but uses the new Send button when secure transmission is desired.

Clicking the secondary "Send" button causes the CM application to validate the sending user's e-mail address with the e-mail address registered during installation (similar to encryption key certificate registration), insert the CM e-mail server address into the "To:" field, move the original destination e-mail address into a hidden field, hide the originally exposed mail header and body of the message and then send the message on to the CM mail server site. The

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

only information transmitted in-the-clear is the e-mail address for the CM mail server. All other information is hidden and secured (by encryption) by the desktop application.

Once the message is received at the CM ASP server, a MD5 checksum is immediately applied to the message and each attachment contained within the message. Next the original address in the "To:" field is reinserted and the entire message is secured with triple DES (3DES) encryption (>128 bit). The ASP server then forwards a notification e-mail that contains a hyperlink to the Secured Socket Layer (SSL) accessible web page of the originally intended recipient. The recipient only has to open the (SSL) hyperlink in the e-mail to be directed to the CM ASP e-mail server.

Opening the link initiates a SSL session that utilizes Rivest-Shamir-Adleman (RSA) encryption to provide the secure link. Once the session is started, the recipient is prompted to enter their e-mail address as their account identification. The recipient also creates their own account password the first time they log into the SSL server. The recipient then uses that password on all subsequent visits.

Once the recipient is successfully logged into the SSL protected session, they are directed to their awaiting 3DES encrypted mail message. The mail message has a MD5 check sum calculated when opened and the sum is compared to the original MD5 check sum. This second MD5 check is performed to ensure, by inference, that the message opened is exactly the same (has not been opened while on the ASP server) as the message that was received. The MD5 check sum is available for the recipient to review at the bottom of the mail message, for additional manual verification.

Opening the message triggers a delivery receipt to be created and sent to the sending party's CM mail account in 3DES encrypted form. It also launches a notification message to the sending party at the e-mail address established during initial registration. The delivery notification message contains a SSL hyperlink to the new message in their CM mail account. Launching the SSL hyperlink initiates a session like the one previously described (above).

Each CM e-mail account archives a copy of each delivery receipt into a permanent e-mail tracking folder. The end user or administrator can simply log into the account and review the message tracking history if the need arises to establish non-repudiation. Also, depending on the delivery option selected, the system can place an expiration time limit on each message.

III. B. The Solution Process Flow

A step-by-step process flow overview of the CM mail model:

1. Certified Mail (CM) initiates an account setup by e-mailing the local user an SSL link to the CM e-mail server.
2. The local user uses the SSL (RSA encrypted) link to log onto the CM certificate server and download the application plug-in.
3. The local installation adds a small proprietary application to the PC. The application is seeded/registered with the e-mail address from step

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1(during download).
4. The application installs a secondary send button on the Outlook tool bar.
5 Users engage the secondary send button when they wish to transmit an encrypted message via the CM ASP interface.
6. The plug-in then executes the proprietary encryption coding within the payload to:

a. Check the seed of the encryption key for user identification.

i. If the e-mail address of the active e-mail account does not match the e-mail address contained in the seed, the message is delivered to an administrator managed folder on the CM SSL server for immediate investigation.

b. Run a proprietary algorithm to check the plug-in integrity. If the integrity of the plug in is found to have been compromised, the tool sends an alert (as in 6. a. i) and prevents further use from that PC.

c. Encrypt the mail header and message fields (only the To: field is left in the clear)

d. Redirect the To: field to transmit the message to the CM e-mail server.

7. The secured message is then transmitted to the ASP server for secure storage until delivery to the intended recipient.
8. Upon message receipt, the CM ASP e-mail server calculates separate MD5 checksums for the message text and each attachment for later use in verifying message integrity during storage on their server.
9. The ASP server transmits an e-mail message to the intended recipient with a SSL link to the encrypted message.
10. The recipient accesses the link to initiate the RSA encrypted SSL session.
11. Once authenticated into the SSL session, the recipient opens the message that has been 3DES encrypted during the entire time it has resided on the ASP database server.

a. The message was 3DES encrypted (CM claims greater than 128 bit, but won't be specific for proprietary reasons) at the time it was received from the sending party, to ensure confidentiality.

b. A MD5 checksum is run against the message upon receipt, but before 3DES encryption, and then again when opened. The two MD5 check sums are compared to ensure the message integrity.

12. While connected to the SSL session, the recipient is able to access the MD5 check sum to manually verify message integrity.
13. The sender receives an e-mail delivery receipt with date, time and checksum stamps. The delivery receipt is also sent to a message tracking folder (in the sender's CM account).

III. C. Meeting & Failing User & Managerial Requirements

During the product evaluation we found that the CM product met many of

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

our user and managerial requirements. Although CertifiedMail did not meet all our requirements, it met enough requirements to be selected for in-house testing. Below are the pros and cons of how CM addressed the user & managerial requirements.

Pros:

1. Message Integrity
    a. The integrity of the local desktop application is validated at each use. Any modifications will change the integrity check sum value and result in application failure.
    b. The active sending e-mail address is validated against the registered e-mail address. Theft or use by any e-mail account other than the registered account will result in application failure.
    c. Theft or attempted unauthorized use will cause the attempted outbound mail message to be directed to a bad e-mail container on the CM ASP system. This action alerts the CM ASP administrator who then alerts the local administrator.
    d. The integrity of each message and attachment is validated by MD5 checksum.
2. Non-Repudiation
    a. A unique user ID based upon e-mail address is required for each user.
    b. Users create their own ASP account password. Internal senders are unable to create passwords for external recipients.
    c. The permanent tracking feature enables Management to historically audit the delivery & reply receipts, match them to the sending and recipient party e-mail accounts and infer non-repudiation by extrapolation
3. Security
    a. Only the CM e-mail address is transmitted in-the-clear (during initial transmission). No other data is transmitted in-the-clear
    b. Each message is encrypted with a 128+ bit 3DES key upon receipt at the ASP server. Encryption is applied using the Microsoft "CryptoAPI" (Cryptography… 4).
    c. The locally executable application is encrypted and designed to fail and notify administrative personnel if altered or used by unauthorized parties.
    d. The recipient can securely reply to the message originator within the SSL browser session.
4. Delivery Receipt/Management Tracking
    a. An encrypted, MD5 checked, and date and time stamped delivery receipt notification is sent back to the internal user. The internal user logs into a SSL secured ASP session to view the tracking history.
    b. Management can create chronologically archived histories of all secured transmissions in order to facilitate auditing.
    c. A copy of the message tracking history remains in the sending

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

party's ASP mail account. Management can set history expiration and administer user accounts on the ASP system on a per user basis.

5. Universal availability
    a. The platform operates on almost all commonly available e-mail and browser setups including WebTV & many wireless internet enabled devices.
    b. Only a valid e-mail client address and a SSL enabled browser are required.
    c. The SSL browser session interface is setup to look and feel like the user is utilizing commonly available web mail clients (Yahoo, Hotmail, EarthLink, etc.). Using this type of well known interface minimizes the need for external user support.
6. Scalability
    a. The CM ASP model allows single user additions as needed.
    b. CM supports conversion from the ASP service model to an on-site CM server based solution when growth dictates.
    c. Scalability provides a declining unit cost model as total units increases, thus providing increasing budget efficiency as the company expands.

Cons:

1. Message Integrity
    a. The message lacks of absolute surety that the encrypted transmission originated from an authorized user. Trust must be placed in CM's proprietary coding, setup and encryption techniques to alert administrators if a problem or compromise occurs.
    b. The MD5 check sum only validates what was received (from the internal user to the CM server) versus what was opened by the recipient. The possibility (though with low probability) exists for transmission interception prior to reception by the CM server.
    c. Implicit trust in placed in the honesty and security of the externally hosted system.
2. Non-Repudiation
    a. Anyone could send secure message from an unattended and unsecured workstation.
    b. Intercepted message could be cracked, though the likelihood of interception is very low.
3. Security
    a. The initial encrypted exchange between internal user and the ASP site is performed with a private, symmetric key. Compromise of that key opens that message and subsequent messages to snooping.
    b. Compromise of the SSL protected account housed on the ASP server gives full exposure to a third party. Users must be vigilant

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

not to expose their account password, lest the account be compromised.

4. Support and Training

a. This solution relies on the internal users to make the correct assessment of when to encrypt e-mail messages.

b. Continual periodic internal training will be necessary to ensure that the users are properly implementing HIPPA e-mail security policy.

c. Managing user accounts and forgotten passwords will be an ongoing issue for the Information Systems staff.

III. D.

The CM solution is compliant with all of the required technical safeguard standards as well as compliant with many of the addressable standards. Access control (unique user IDs and emergency access), audit controls, and user authentication are the "required" (US Dept…164.312) safeguards. Transmission security, data integrity, and the automatic logoff and encryption features of access control are the "addressable" (US Dept…164.312) safeguards of The Security Rule.

CM complies with the access control standard of the 'required' safeguards by establishing unique user (accounts) IDs based upon e-mail address and also enables emergency access to each of those accounts. Audit controls are facilitated by the message tracking archive that is accessible by individual user or the system administrator. User authentication is established at the beginning of each SSL session by logging into the password protected account. Authentication is also established at each use of the desktop application by authenticating that the active e-mail account is the same as the ID established during registration/account creation.

CM meets the transmission security and data integrity standards of the 'addressable' safeguards by encrypting with both proprietary and 3DES 128+ encryption tools, creating a RSA secure SSL session for message access and running MD5 checksums on the message and each attachment. The CM solution also satisfies the addressable automatic logoff specification by automatically terminating the SSL session after 10 minutes of inactivity.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Conclusion

HIPAA regulations impact e-mail transmissions in almost every area of the health care field. As small health care businesses grow, so do the challenges of their HIPAA compliance efforts. The health insurance provider examined by this paper has recently experienced the challenge of addressing its e-mail privacy and security compliance due to the rapid growth of the business. Initially there was no data integrity, policy control, validation or managerial auditing of the transmission of EPHI related e-mail. The company clearly had a growing HIPAA e-mail privacy & security compliance issue.

I began by reviewing the HIPAA regulations and professional legal opinion to establish the appropriate parameters to securing EPHI e-mail. I then identified the legal risks and technical vulnerabilities of an unsecured EPHI transmission. I followed by finding the most cost-effective intersection of legal, managerial and user requirements.

I informed company management of the strengths and weakness of the proposed solution and established the need for continual personnel training to manage the inherent weakness of the solution.

The ASP service based security solution met the five technical safeguards requirements of the HIPAA Final Security Rule and the conformed to the standards of the HIPAA Privacy Rule while also fulfilling a majority of user and managerial requirements. The result is a secure e-mail transmission system that significantly increases the security EPHI transmission while substantially reducing the probability of DHHS imposed HIPAA fines.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

CertifiedMail.com. 2004. CertifiedMail Corp.
http://www.certifiedmail.com (20 Mar. 2004).

"Cryptography and PKI Basics". Microsoft TechNet. 5 July 2000.
Microsoft Corporation.
http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/cryptpki.mspx?pf=true (1 April 2004).

Grove, Tom. "Summary Analysis: The Final HIPAA Security Rule".
HIPAAdvisory.com. 2002-2003. Phoenix Health Systems.
http://www.hipaadvisory.com/regs/hipaaprimer.htm. (24 Mar. 2004).

"HIPAA Primer". HIPAAdvisory.com. 2002-2003. Phoenix Health Systems.
http://www.hipaadvisory.com/regs/hipaaprimer.htm (24 March 2004).

"Is a Business or Agency a Health Care Clearinghouse?: Covered Entity
Decision Support Tool". Centers for Medicare & Medicaid Services.
U.S. Dept. of Health & Human Services
http://www.cms.hhs.gov/hipaa/hipaa2/support/tools.decisionsuppprt/xmldecision.asp?decision=D2 (31 Jan. 2003).

Maiwald, Eric. "Are Computer Viruses Getting Worse?".
HIPAAdvisory.com. Jan 2002. Phoenix Health Systems
http://hipaadvisory.com/action/secureQA/Secure01.htm (18 March 2004).

National Institute of Standards and Technology. Special Publication 800-33;
Underlying Technical Models for Information Technology Security.
Washington: U.S. GPO, 2001 (17 March 2004).

"Privacy, Security and HIPAA; A Common Sense Approach to Meeting HIPAA
Standards". Authora.com. 2004. http://www.authora.com (24 Mar. 2004.)

Salamone, Salvatore. "Getting Serious About HIPAA Compliance".
Bio-ITWorld.com. 10 Mar. 2003.
http://ww.bio-itworld.com/news/031003_report2161.html (28 Mar. 2004).

Shannon, Heather. "W32.Beagle.E@mm". 28 Feb 2004.
Symantec Security Response.
http://securityesponse/symantec.com/avcenter/venc/data/w.32.bagle.e@mm.html (31 March 2004).

"Small Companies Need to Act on HIPAA Rules".

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

SmallBusinessComputing.com. 18 Feb. 2004. Jupiter Media Corporation. http://www.smallbusinesscomputing.com/news/article.php/3313751 (26 Feb. 2004).

Spohn, Darren. "HIPAA and the Small Business". Network World Fusion.com 8 Mar. 2004 Network World Fusion. http://nwfusion/com/net.worker/columnists/2004/0308techpartners.html (8 Mar. 2004).

U.S. Department of Health and Human Services. Standards for Privacy of Individually Identifiable Health Information: 45 CFR Parts 160 and 164. Washington: U.S. GPO, 2003. (21 Feb. 2004)

Wachler, Andrew B., and Fehn, Amy K. 2004. HIPAA-Attorneys.com. 29 March 2004. Wachler & Associates, P.C. http://wachler.lawoffice.com.hipaa.htm (29 Mar. 2004).

Weil, Steven. "HIPAA Security Rule: What It Is & How to Comply With It". Security Focus.com. 1 Mar. 2004. http://www.securityfocus.com/infocus/1764 (9 Mar. 2004).

"ZipLip-HIPAA Security Rules Matrix". ZipLip.com. 2003. ZipLip, Inc. http://www.ziplip.com. (9 Mar. 2004).

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.