Global Information Assurance Certification Paper

Scrambled Eggs: A HIPAA Compliance Recipe for Data Encryption

HIPAA Security Rule - Technical Safeguards.
Transmission Security “Encryption”
§ 164.312(e)(2)

GIAC HIPAA Security Certificate (GHSC)

Practical Assignment:

Version 2.0

Submitted by: Steven Tate

March 17, 2005

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Abstract:

It is intended that this paper serve to explain the addressable encryption implementation of the Technical Safeguard – Transmission Security Standard. In addition, it will also serve as the practical assignment, submitted in partial fulfillment for the HIPAA Security Implementation Certificate (GHSC). The following encryption explanation is specifically rooted in the HIPAA Security Standards final rule[1], prompting a clear understanding of encryption implementation during the transmission of Electronic Protected Health information (EPHI) traversing "open" insecure networks. The ensuing policy evaluation (Option B) will provide a sample policy which can be used to ensure compliance. This evaluation is then followed by procedures that can be implemented by an organization to comply with the HIPAA encryption standard.

Introduction:

Throughout history, from ancient civilizations and to modern day man, the employment of some form of encryption is necessary to ensure secrecy of communications. Both senders and receivers of the communiqué often go to great lengths to secure information delivery, integrity, and confidentiality. Long before the ratification of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and its mandated implementation date of April 21, 2005,[2] healthcare organizations have struggled with the quandary of how to best protect sensitive data during transmission. The use of encryption is a security method to achieve this goal.

Encryption is the result of plain text information being subjected to a complex mathematical process where an algorithm/cipher is applied to it. The result is the scrambling of plaintext it into unreadable ciphertext. However, as with any mathematical processes it can be reversed or deciphered. Once the corresponding decipher process is applied to the ciphertext, it would then revert to decrypted (readable) plain text.

A cornerstone of the encryption process is a "secret key" which is used by trusted parties to encrypt and decrypt communications. Encryption key length is measured in bits, which is directly proportionally to the strength of encryption algorithm. Consequentially, the more bits in the key, the stronger it is and harder for outsiders to break. There are many types of encryption formats each with their own attributes of applicability. Attributes of two common cryptography keys include:

Symmetric Key Encryption – A traditional form of cryptography using a single key by both sender and receiver to encrypt and decrypt information.

Asymmetric Key Encryption – Using two keys whereby users have a public and a private key. The public key is made public, but the private key remains

secret. In this method information encrypted with the public key can only be decrypted with the use of a private key[3].

The HIPAA security rule sets forth standards implementations (required and/or addressable), that Covered Entities (CE) shall provide to all Electronic Protected Health Information (EPHI) that it possesses, comes in contact with, receives or transmits[4]. At a very minimum the covered entity is to provide:

- Data confidentiality and integrity
- Protection against any reasonably anticipated threats
- Protection against any reasonably anticipated use or disclosures
- Workforce compliance documentation

A generally accepted industry practice of protecting data during transmission is a requirement encompassing the use of various encryption technologies[5].

HIPPA is now law. The ramifications of compliance failures and wrongfully disclosed (compromised) electronic protected health information can bring penalties to organizations as well as individuals. Sanctions may consist of small fines if the offense falls under SEC. 1176 (a). However, the incident maybe so egregious that under SEC. 1177 (a), imposed penalties may include fines up to several hundred thousand dollars and possible prison sentences[6]. Moreover, the exposed organization will surly realize a damaged reputation in the eye's of the general public, whereby this unfavorable perception could lead to a loss of customer confidence and future business. It is quite discernable that it is in the best interest of both the public and private sectors that the HIPAA implemented be complied with.

Assignment 1 - Explanation

This paper delves into HIPAA Security Standard, Technical Safeguards – Transmission Security §164.312(e) (1)[7], specifically focusing on the addressable encryption implementation specification (e)(2)(ii). Healthcare organizations of all sizes and functions have both a fiduciary duty and a legal obligation to protect electronic protected health information received viewed, stored, and transmitted while in its possession[8].
Prior to the mandated HIPAA compliance date of April 2005, healthcare organizations most often employed a set of industry best practices with regard to information security, and data encryption. The HIPAA final rule provides encryption guidelines with a unique spirit of confirmatory vagueness, allowing for individual interpretation designed to cover healthcare organizations of all sizes and budgetary constraints.

Upon close examination of the HIPAA rule, one can clearly see that it is constructed to ensure that covered entities, clearing houses, and third parties in the health care industry provide security safeguards to protect the confidentiality,

integrity and availability of electronic protected health information.[9]

The standard and implementation state that healthcare organizations "implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network[10], and to implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."[11]

The purpose of this paper is to explain the meaning and illustrate the intent of the encryption implementation specification, as it applies to protecting EPHI transmitted via insecure and/or open networks. Insecure transmission mediums such as the Internet, wireless LANS/WANS, and remote access (Dial-up & VPN) via the Internet are areas targeted by the encryption implementation specification. It should be noted that wireless technologies are not specifically identified in the final HIPAA security rule. It is the understanding of this author that encryption of EPHI utilizing wireless technologies as a transmission medium is deemed appropriate, and falls within the intent of the definition of "insecure" networks.

When consideration the aforementioned thoughts, one is left with answering the questions of: Is there a specific encryption standard or mechanism to be deployed, and what does "deemed appropriate" really mean? Fortunately the final rule addressed encryption mechanisms by declaring a position of neutrality, not specifying any type and/or strength. The non specificity of the rule may lead to uncertainties regarding encryption implementation within the healthcare industry. This was not the intent of the final rule. Covered entities are to perform a risk analysis to determine exposure and severity. The risk analyses, and other factors, are to be used to determine the appropriate encryption algorithm and strength. The intent is to allow covered entities the freedom to consider industry best practices, and the uniqueness of their environment in selecting encryption type and strength.

As of this writing, encryption types Advanced Encryption Standard (AES), Triple DES (TDES), and IPSec are popular choices primarily due to cryptographic key strengths and symmetric block ciphers.[12],[13] HIPAA does not mandate the use of specific encryption infrastructure devices (Routers, Firewalls, VPN concentrators, etc). It does this to reinforce its technology neutral position[14]. Again this place's the covered entity in the unique position to determine infrastructure encryption implementations based on network risk analysis, existing infrastructure, and technical staffing. The rule also points out that with rapidly changing technology, it would be impractical and inappropriate to name a specific type and strength[15]. It should be noted that although the covered entities risk analysis determines the encryption type, all implemented

protections should be commensurate with perceived risks. However, where risk of exposure and/or interception is significant, encryption is expected.

Answering the question of what is "deemed appropriate" is based on weather or not electronic protected health information is being transmitted over open (unprotected), or insecure (weakly protected) networks. Risk analysis, financial costs, and required technical resources are factors to consider when determining if encryption implementation is appropriate.

HIPAA makes distinctions between small, medium, and large organizations. Regardless of its size, implementing data protection technologies and their associated components (hardware & software) is often very expensive. The task of protecting data while simultaneously maintaining cost efficiencies is a delicate balancing act. Universal mandates may prove to be out of proportion for the required level of protection, and therefore cost prohibitive. It is my understanding that this is not the intent of the final rule. The final rule is constructed in a manner as to not place financial burdens on entities of any size. Nevertheless, adherence to industry best practices clearly demonstrate that if a covered entity is transmitting EPHI over the internet and/or wireless networks, it is therefore "deemed appropriate" and should be encrypted.

The encryption implementation specification is designated "addressable". The intent here is for the CE to address the issue of encryption; however it does this with more flexibility in determining implementation. For example, email encryption is encouraged but not mandated. This is because there is no simple and/or interoperable method.[16] The final rule's flexibility allows the CE to:

- Implement the specification if reasonable and appropriate.
- Implement an alternative measure if reasonable and appropriate and document how it meets the standard.
- Implement no additional security measure if the specification is not implementing the standard and document why it would not be reasonable and appropriate to implement the standard.[17]

Finally, the final rule briefly touches on the issues of alarm capabilities, audit trails, entity authentication, and event reporting. It was determined that these activities are not required because most telecomm providers provide these services. It should be noted that these issues have been removed and are no longer part of the final rule.

Assignment 2 – Policy evaluation (Option B)

1.0 Purpose

To establish a strategic plan to ensure appropriate and secure encryption technologies are afforded to all Electronic Protected Health Information (EPHI), traversing Tate Medical Systems networks and network sub-systems. To provide direction on the use of nonproprietary encryption algorithms/ciphers, ensuring data confidentiality and integrity will not be comprised.

2.0 Guidelines

This document is to serve as a guideline for HIPAA compliance, specifying information technology encryption standards that support information system life cycle activities for Tate medical Services.

3.0 Scope

The standards apply to all Tate Medical System's employees in its entirety, or separately to contractors responsible for EPHI transmitted on insecure network systems. The standards apply to all existing implementations, and new installations. The standards are to be used as blueprint facilitating the system-wide migration to a standards-based environment.

4.0 Policy

It is the policy of Tate Medical Services IT Department, to encrypt any and all EPHI transmitted over insecure networks such as the internet, and wireless LAN/WAN environments. Employed encryption technologies will incorporate the use of approved, proven, and nonproprietary Symmetric algorithms such as AES, 3DES, or RC4 with minimum cipher key lengths of 128 bits. In addition, an approved HASH (checksum) verifying data integrity will be integrated into this policy.

As of the writing of this document, the only approved algorithm and hash to be implemented are AES and SHA-1 respectively. The use of unapproved or proprietary encryption algorithms (Symmetric and/or Asymmetric), and hashes is strictly forbidden. On an annual basis, a Tate Medical Systems Technical Advisory Team will review encryption and hashing technologies, suggesting any enhancements deemed appropriate.

5.0 Maintenance of the Standard

This document is maintained by the Chief Information Officer with input provided by IT Engineers of Tate Medical Services. This document is to be updated annually, or as directed by the Technical Advisory Team.

6.0 Enforcement

With the approval of Tate Medical Services Chief Security Officer and the Director of Human Resources, all Tate Medical Services employees and contractors are responsible for explicit adherence of the aforementioned policy. Any violation or unapproved deviation form this policy may result in disciplinary actions; up to and including termination of employment.

7.0 Distribution

Director of Human Resources
Chief Information Officer
Chief Security Officer
Director, Network Services
Technical Advisory Team members
Manager, Network Services
Manager, Technical Systems
Manager, Desktop Support

8.0 Acronyms and definitions

3DES: Triple Data Encryption Standard, an encryption mechanism of 168 bits
Asymmetric: an encryption technology employing the use to two cipher keys (public and private) to encrypt and decrypt information.
AES: Advanced encryption standard, a strong encryption technology with bit lengths of 128, 192, and 256 bits in length.
Checksum: a mathematical method of verifying bit accuracy.
Chief Information Officer (CIO).
Encryption: a method of turning plain text data into unreadable cipher text.
Hash: A systematic method to ensure the integrity (lack of change) of data in transit.
Information Technology (IT)
LAN: Local Area Network. A network infrastructure that is internal to an organization.
Proprietary encryption: A specific encryption mechanism not adhering to industry acceptable standards.
RC-4: an encryption mechanism/cipher of 128 bits in length.
SHA-1: Secure Hash 1, a cryptographic hash used to ensure the integrity of data.
Symmetric: an encryption technology employing the use of a single

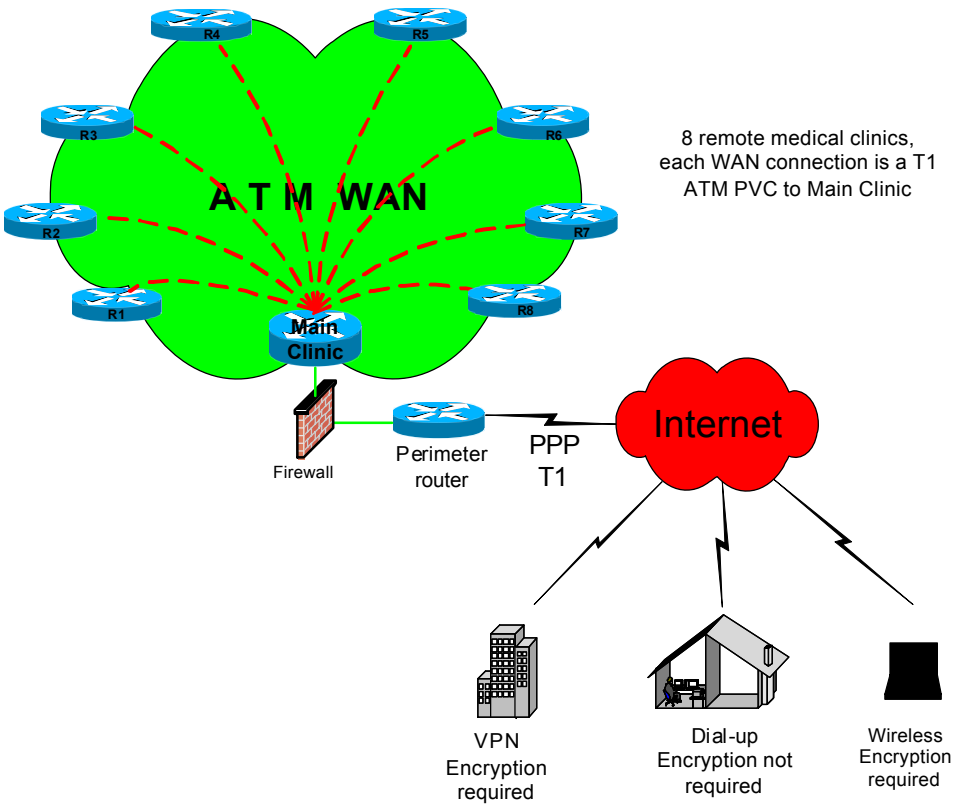
cipher key by both sender and receiver encrypt and decrypt information.
Technical Advisory Team (TAT)
VPN: Virtual Private Network, a technology for securing network connections over insecure networks.
WAN: Wide Area Network. A network infrastructure that is external to an organization.

9.0 Revision history

Assignment 3 – Procedures (Option B)

The following is based on the fictitious organization Tate Medical Services (TMS). TMS is a collective group of specialized clinics with a patient base of approximately 10,000. All clinics are out patient care facilities serving a small to medium demographic area. The Main clinic serves as an aggregation point for medical service activities, as well the home for billing and human resources. TMS's infrastructure is a homogeneous network comprised of Cisco Systems equipment, where the security and/or encryption policy and procedures are base on industry best practices.

This section describes the characteristics of the environment and procedures needed to implement TMS's transmission encryption policy, protecting EPHI on insecure networks. The following procedures are specifically focused on the multifunction firewall and is relative to the way the EPHI is transmitted thought TMS.



As detailed in the above figure TMS network topology consists of eight remote clinics, each connecting to the Main clinic via T1 WAN PVC to the Main clinic. As a traditional hub and spoke ATM network, each internal site-to-site connection is essentially point-to point. TMS has a PIX firewall which performs granular traffic filtering, VPN tunneling, and packet encryption. It also has a perimeter router that is the traffic demarcation point, segregating the internal LAN form the external WAN. It is here that the connection to the internet is made and the router is configured to perform basic security and ingress/egress traffic filtering.

These ATM WAN circuits are secure point to point connections, and therefore not subject to the encryption implementation stipulated in the final rule. As shown, TMS allows remote connectivity to covered entities, dial-up, and wireless users, who transmit traffic via an insecure network (internet). The following procedure is to be used for demonstration purposes only, and should not be interpreted as a representative and/or functional encryption configuration. Encryption compliance configuration procedures included are: site to site, VPN, and dial-up. It is assumed that the wireless connection points (hotspots,

airports, etc.) will have at a very minimum have WPA encryption activated, SSID broadcasting and MAC address filtering disabled. To provide encryption for electronic protected health information, TMS will not need to purchase encryption hardware or software (clients). The following procedures will demonstrate how to configure the Pix firewall to encrypt EPHI traffic for each of these configurations as well as the necessary client end points.

- Site to site
- VPN Wireless connections
- Dial up links
- Client end points

Configure the Cisco PIX firewall for Encryption
Section 1 – Site to Site Encryption

Step 1

Make sure the firewall the appropriate licensing for the required amount of encryption.
On the command line type in:
Show run:

VPN-DES: Enabled
VPN-3DES-AES: Enabled
IKE peers: Unlimited

This read out shows the firewall is capable of performing VPN, TDES, and AES encryptions. From this point on all configuration commands are performed in the privilege “config” mode.

Step 2

Set the system time and enable logging.
On the command line type in:

```
Clock set 15:30:00 March 17 2005
clock timezone pdt -8
ntp server 10.10.10.10
logging on
logging timestamp
logging host inside 10.10.10.3
logging facilty 23
```

```
logging trap critical
logging history debugging
logging history buffered debugging
ip audit attack action alarm
```

Step 3

Configure the firewall to permit the IPSec protocol
On the command line type in:

```
sysopt connection permit-ipsec
```

Step 4

Configure the firewall for the crypto map. This step maps a crypto map name to the ACL, the remote peers address, the transform-set (encryption and hashing)
On the command line type in:

```
crypto ipsec transform-set Tate_Medical_Services esp-aes esp-sha-hmac
crypto ipsec security-association lifetime seconds 3600
crypto map TMS 30 ipsec-isakmp
crypto map TMS 30 match address 130
crypto map TMS 30 set peer 200.214.138.67
crypto map TMS 30 set transform-set Tate_Medical_Services
crypto map TMS interface outside
```

Step 5

This step enables the IPSec policy, configures the interface, the DSS (Digital Signature Standard) public key, and establishes the encryption type and hash to be used between the peers.

On the command line type in:

```
isakmp enable outside
isakmp key ******** address 16.114.238.6 netmask 255.255.255.255 no-
xauth no-c
isakmp identity address
isakmp policy 30 authentication pre-share
isakmp policy 30 encryption aes-256
isakmp policy 30 hash sha
isakmp policy 30 group 1
isakmp policy 30 lifetime 0
```

Step 6

Configure the Per-session Encryption Policy
On the command line type in:

```
access-list 130 permit ip host 172.X.X.172 150.150.150.0 255.255.0.0
```

Section 2 – VPN Encryption

Step 1

Create a VPN address pool, the DNS, Wins and default domain.

```
ip local pool tmsvpn2 10.13.15.10-10.13.15.254
vpngroup 3000client idle-time 1800
vpngroup TMS address-pool tmsvpn2
vpngroup TMS dns-server 10.10.10.65
vpngroup TMS wins-server 10.10.10.66
vpngroup TMS default-domain TMS.TMS.org
vpngroup TMS idle-time 1800
vpngroup TMS password ********
```

Step 2

Configure the firewall for the VPN crypto map. This step maps a crypto map name to the ACL, the transform-set (encryption and hashing)
On the command line type in:

```
crypto ipsec transform-set VPN_TMS esp-aes esp-sha-hmac
crypto ipsec security-association lifetime seconds 3600
crypto map VPN 20 ipsec-isakmp dynamic VPN_TMS
crypto map VPN 20 client configuration address respond
crypto map VPN 20 client configuration address initiate
crypto map ipsec-isakmp dynamic VPN_TMS
crypto map VPN 20 ipsec-isakmp
crypto map VPN 20 match address 20
crypto map VPN 20 set transform-set VPN_TMS
crypto map VPN interface outside
```

Step 3

This step enables the IPSec policy, configures the interface, the DSS (Digital

Signature Standard) public key, and establishes the encryption type and hash to be used between the peers.

On the command line type in:

```
isakmp enable outside
isakmp key ******** address 0.0.0.0 netmask 0.0.0.0 no-xauth no-c
isakmp client configuration address-pool local VPN_TMS outside
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption aes-256
isakmp policy 20 hash sha
isakmp policy 20 group 1
isakmp policy  lifetime 0
```

Step 4

Configure the ACL VPN Encryption Policy
On the command line type in:

```
access-list 20 permit ip any any 255.255.0.0
```

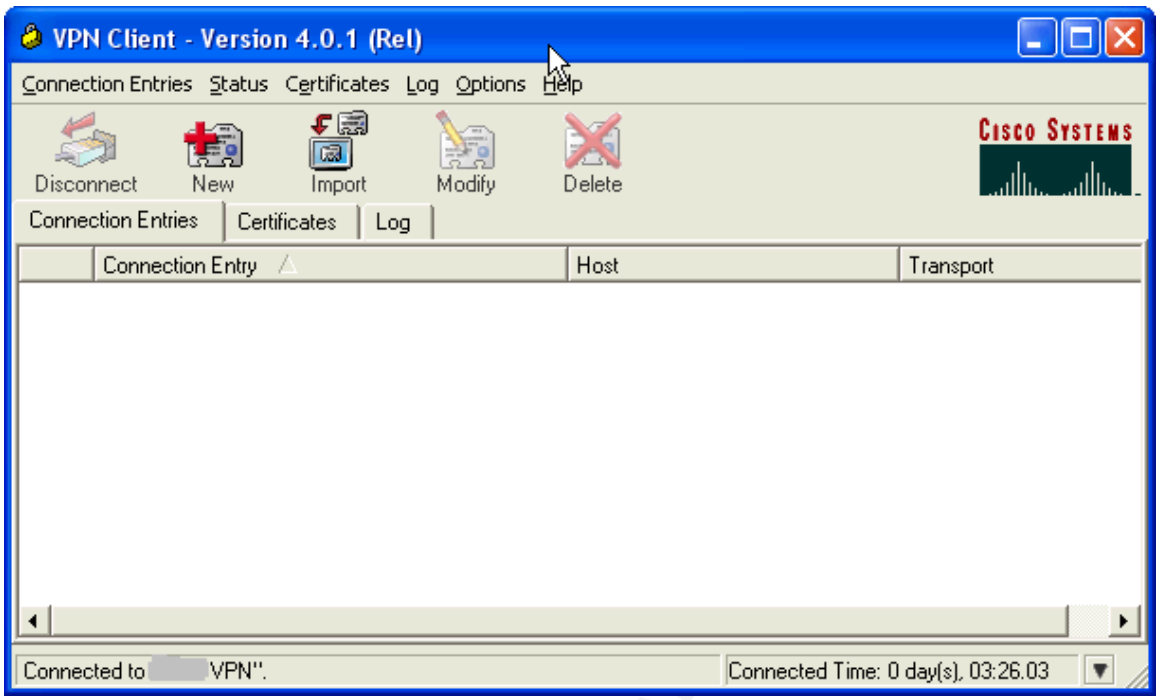
Section 3 – Dial-up VPN Encryption
Not necessary

Section 4 - Configure the VPN on the Client
Step 1

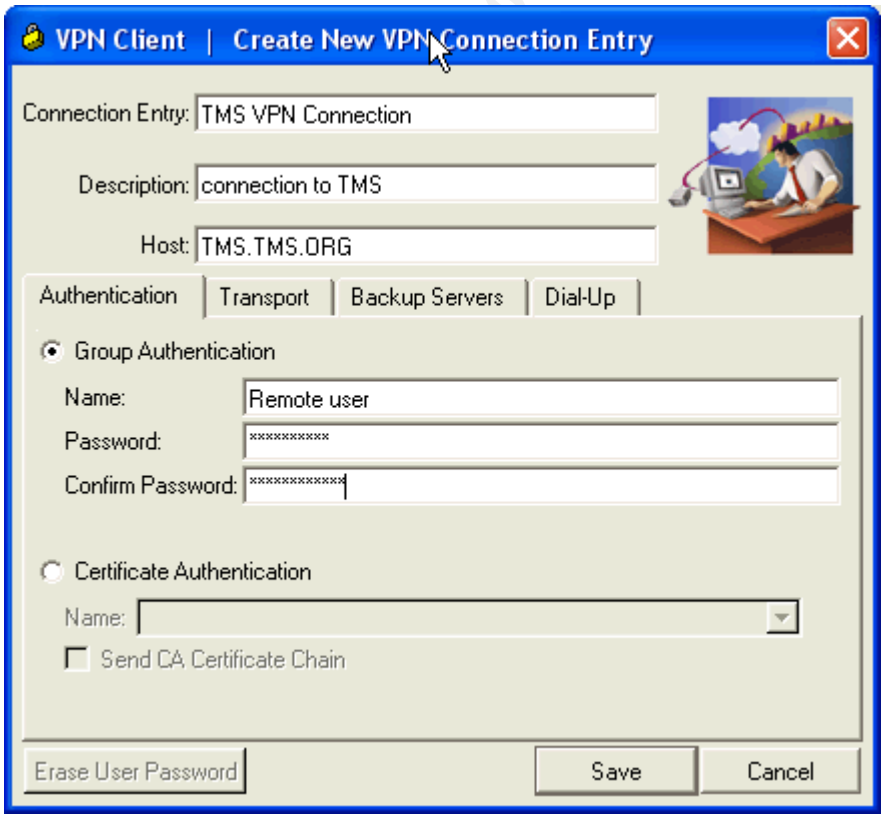
On client end points install Cisco VPN client 4.0 software.

Step 2

After launching the VPN client application, it must be configured to communicate securely with the PIX. A two phase encryption connection must be established and maintained for the duration of the connection. On the VPN client window select new.



When the create new VPN connectivity window comes up, fill in the information fields as directed by the IT department. Once this is done, select save and in the next window click connect. From this point a secure encrypted connection will be established to TMS.



Summary

As mentioned earlier “HIPAA is now law.” The final rule does not mandate encryption of EPHI, however industry best practices govern the necessity of covered entities of using encryption to protect data. This submission addressed the Encryption implementation specification. By using a fictitious and real world example of a health care network infrastructure, it was demonstrated that a well documented environment, establishing a written policy, and following the listed procedures will allow the organization to implement encryption on insecure networks in total HIPAA compliance.

References:

[1] Department of Health and Human Services, 45 CFR Parts 160, 162, and 164, Health Insurance Reform: Security Standards; Final Rule
Federal Register/ Vol. 68, No. 34/Thursday, February 20, 2003/ Rules and Regulations 8356, 8357

[2] Baumler, Julie, et. al. HIPAA Security Implementation, ver. 2.0, SANS Press, December 2004,

[3] Hansche, Susan, et.al, Official (ISC)2 Guide to the CISSP Exam, (ISC)2 Press 2004

[4] Baumler, Julie, et. al. HIPAA Security Implementation, ver. 2.0, SANS Press, December 2004

[5] ISO/IEC 17799:2000, Code of Practice for Information Security Management, Part 1, 10.3.2

[6] Public Law 104-191 AUG. 21, 1996, Health Insurance Portability and Accountability Act of 1996
104th Congress
http://aspe.hhs.gov/admnsimp/pl104191.htm

[7] Department of Health and Human Services, 45 CFR Parts 160, 162, and 164, Health Insurance Reform: Security Standards; Final Rule
Federal Register/ Vol. 68, No. 34/Thursday, February 20, 2003/ Rules and Regulations 8356, 8357

[8] ibid

[9] ibid

[10] Ibid.

[11] Baumler, Julie, et. al. HIPAA Security Implementation, ver. 2.0, SANS Press, December 2004

[12] National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication (FIPS PUB 197), November 26, 2001

National Institute of Standards and Technology (NIST), special publication 800-67, April 16, 2004

http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[13] Mason, Andrew, Cisco Secure Virtual Private Networks, Cisco Press, 2002

[14] Department of Health and Human Services, 45 CFR Parts 160, 162, and 164, Health Insurance Reform: Security Standards; Final Rule
Federal Register/ Vol. 68, No. 34/Thursday, February 20, 2003/ Rules and Regulations 8356, 8357

[15] ibid

[16] ibid

[17] Baumler, Julie, et. al. HIPAA Security Implementation, ver. 2.0, SANS Press, December 2004