Global Information Assurance Certification Paper

Curt Purdy
GIAC HIPAA Security Certificate GHSC
Practical Assignment Version 1.0 Option B
Second Attempt
March 15, 2005

Procedures for Establishing Encryption Controls on Transmitted Electronic Protected Health Information

HIPAA Security Rule, Technical Safeguards, § 164.312(e)(1)(ii)

Abstract

Messages and data are passed back and forth across on all networks including the Internet. As such, these messages and data are susceptible to compromise by various means from network sniffing to man-in-the-middle attacks. In all health-care organizations, much of these messages and date are made up of Electronic Patient Health Information (EPHI).

Covered Entities (CE) are covered by HIPAA Security Rule, Technical Safeguards, 164.312(e)(1) and must guard against unauthorized access to EPHI that is being transmitted over an electronic communications network according to the standard rule. It must implement a mechanism to encrypt EPHI whenever deemed appropriate by the addressable encryption implementation rule.

This paper will cover the policies and procedures necessary for GIAC Health, a mid-sized regional MHMR center, to comply with this rule. An explicit written policy that will enforce the rule will be given along with the procedures necessary to meet that policy for the devices, environment, and transmission methods used by GIAC Health.

Table of Contents

Table of Figures

Table of Tables

Assignment One: Define the Environment

GIAC Health is a mid-sized regional MHMR center based in Austin, Texas with 4 main branches connected with point-to-point T1 lines in Austin, San Antonio, Round Rock, and Georgetown and 12 sub-branches scattered in and around Austin connected with wireless 802.11b and VPN concentrators.

The main enterprise server is an AS/400 that holds the database containing the major portion of EPHI. The AS/400 has a partition running Windows 2000 Server and runs the enterprise application that accesses that data. Access to that data takes five forms:

1) Locally, dumb terminals over twin-ax cable, and Linux workstations running telnet sessions, and Windows 2000 Professional workstations running client terminal, some with Internet access connect to the AS/400 in native OS/400 mode over Ethernet.
2) Locally, Windows 2000 Professional workstations access the Windows based enterprise application with a proprietary client.
3) Remotely, the main and sub-branches access the data with Linux and Windows workstations over T1 and wireless.
4) Remotely, single users consisting of doctors and staff access through dial-up lines on the core router. There are firewall rules between the dial-ups and the core router.
5) Remotely, single users access from the Internet through VPN clients on their workstations.

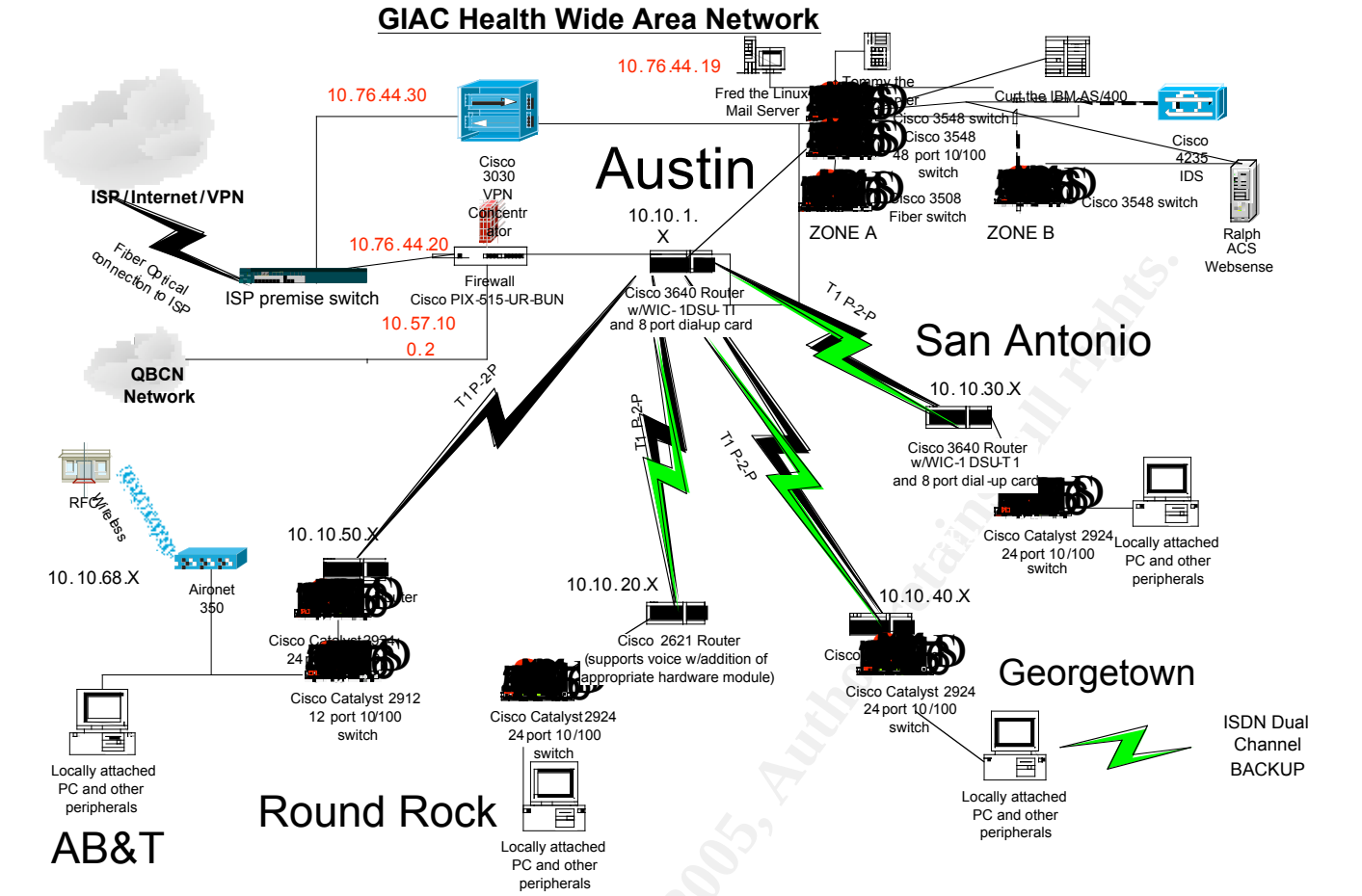
In addition all Internet access is through the primary DS3 line at the main facilities. No external Internet connections are permitted at any of the branches, and split tunneling is disallowed at the VPN client-end.

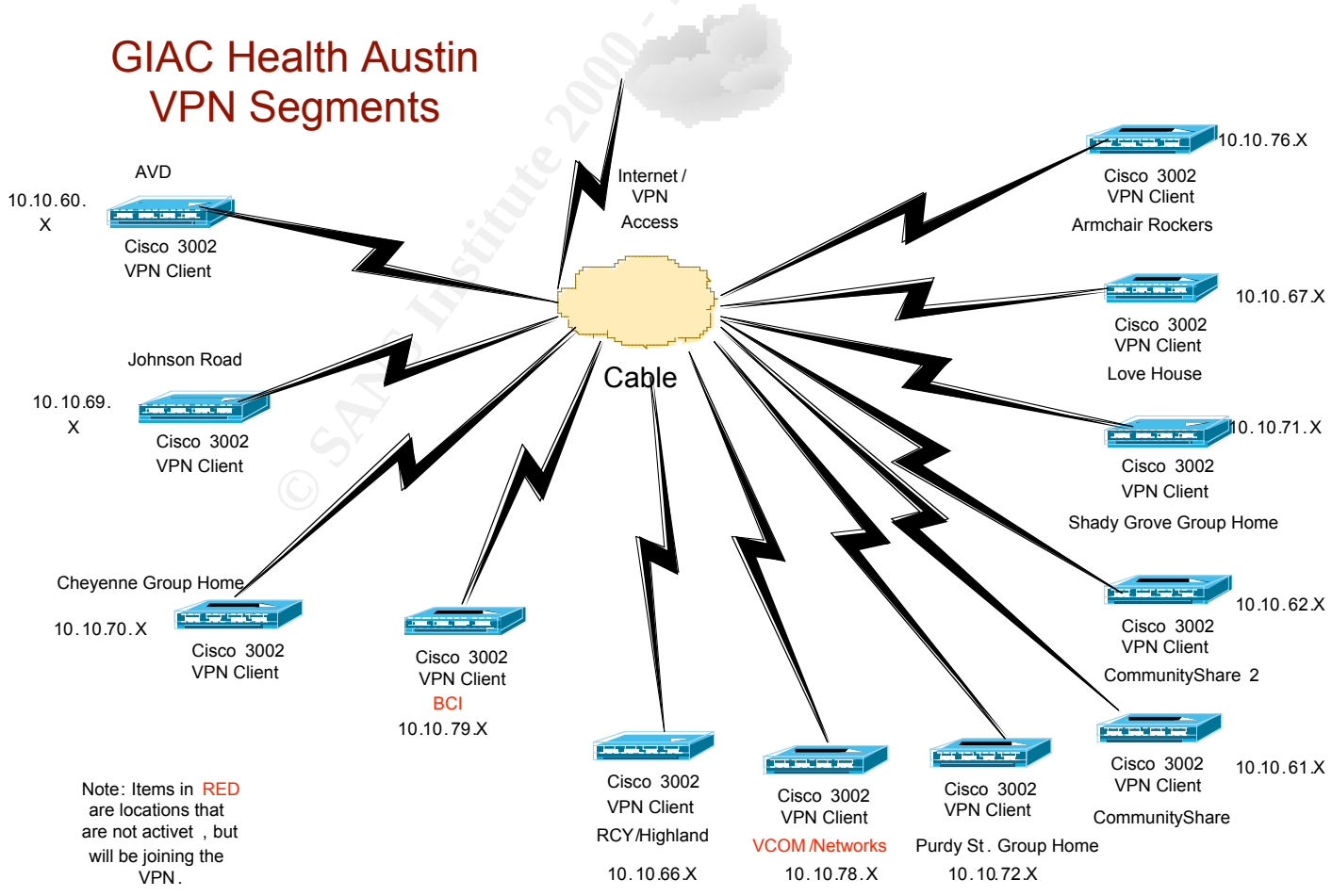
In addition to the AS/400 access, the main facilities house a SuSE Linux 9.1 mail and web servers as well as a Windows 2003 file and print server. Access both internally and externally occur through VPN as described above. In addition, the mail and web servers are accessible from the Internet with email clients and web browsers through static NATing in the firewall.

There is a Network Intrusion Detection System in-line with the Internet and on a span-port on the bank of internal switches, capable of seeing all traffic both internal and external on the WAN as well as from the Internet. The public is allowed access to the web browser from the Internet, and staff are allowed POP3 access to the mail server from the Internet without VPN.

EPHI is sent and received across the Internet through email, FTP, and web-based applications as well as across POTS through the dial-up lines on the

router. EPHI is also printed and faxed and sent and received by mail courier as well as by doctors and staff.





Assignment Two: Explanation

Almost all the final HIPAA security rules have one thing in common, and that is to protect the confidentiality, integrity, and availability of EPHI. 164.312(e)(1) addresses two of the three as it concerns transmission of EPHI over electronic networks. Encryption can be used to insure both the confidentiality and integrity of data. The rule states:

Covered Entities (CE) are covered by HIPAA Security Rule, Technical Safeguards, 164.312(e)(1) :

> **§ 164.312 Technical Safeguards**
>
> (e)(1) *Standard: Transmission security*. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
>
> (2) *Implementation Specifications*
>
> (ii) *Encryption* (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

The development of this standard to the final rule is interesting. As stated in the announcement of the final rule by the Department of Health and Human Services where comments and responses were given:

Under "Technical Security Mechanisms to Guard Against Unauthorized Access to Data that is Transmitted Over a Communications Network," we proposed that "Communications/network controls" be required to protect the security of health information when being transmitted electronically from one point to another over open networks, along with a combination of mandatory and optional implementation features. We proposed that some form of encryption must be employed on "open" networks such as the internet or dial-up lines.[1]

They received numerous comments on this, particularly from the small practices as to the onerous nature of these demands that the department softened the rule:

Thus, we agree that encryption should not be a mandatory requirement for transmission over dial-up lines. We also agree with commenters who mentioned the financial and technical burdens associated with the employment of encryption tools. Particularly when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting e-mail communications with patients. As a result, we decided to make the use of encryption in the transmission process an addressable implementation specification. Covered entities are encouraged, however, to consider use of encryption technology for transmitting electronic protected health information, particularly over the internet. [1]

How can CE's protect the confidentiality, integrity, and availability of EPHI? As for when EPHI is transmitted across electronic networks, there are various forms of encryption available to protect that information. Basic encryption itself comes in a number of flavors.

The National Institute of Standards and Technology (NIST) endorses the advanced encryption standard (AES) by Rijndael. In addition there are a number of other algorithms considered very secure such as Blowfish and 3DES. Although it is arguable that these ciphers can be broken with more powerful computers, at least for the foreseeable future this would take anywhere from years to centuries to do even with the most powerful computers today.

As for end-to-end connections, various forms of virtual private networking (VPN) exist. IPSec VPN's are very popular and can use any of the above encryption methods along with both MDA5 and SHA1 hashing algorithms to "tunnel" data between endpoints by encrypting each packet as it leaves the sender until it arrives at the receiving point.

There are two forms of IPSec, Authentication Header (AH) and Encapsulation Security Payload (ESP). AH full tunnels the entire packet which is the most secure method, but this causes problems with many NAT systems because the header information is obscured. ESP relieves this problem by not encrypting the packet header. Another protocol Internet Key Exchange (IKE) negotiates the session to form the Security Association (SA). Once the SA is established, data can be exchanged through the tunnel.

Other forms of VPN exist such as SSL-based and MPLS-based VPN.

Table 1. MPLS, IPSec, and SSL Comparison[2]

	MPLS-Based VPN	IPSec-Based VPN	SSL-Based VPN
Topology	Site-to-site VPN: Hub-and-spoke or full-mesh	Site-to-site VPN: Mainly hub-and-spoke	Remote-access VPN
Security Session authentication	Establishes VPN membership during provisioning, based on logical port and unique route descriptor Defines access to a VPN service group during service configuration; denies unauthorized access	Authenticates through digital certificate or preshared key Drops packets that do not conform to the security policy	Authenticates through digital certificate
Confidentiality	Separates traffic, which achieves same results delivered in trusted Frame	Uses a flexible suite of encryption and tunneling mechanisms at the IP network layer	Encrypts traffic using the public key infrastructure (PKI)

	Relay or ATM network environments	IP network layer	infrastructure (PKI)
QoS and SLAs	Enables SLAs with a scalable, robust QoS mechanism and traffic-engineering capability	Does not address QoS and SLAs directly, although Cisco® IPSec VPN deployments can preserve packet classification for QoS within an IPSec tunnel	Not applicable; service provider network is unaware of SSL traffic
Scalability	Highly scalable because no site-to-site peering is required Capable of supporting tens of thousands of VPNs over the same network	Acceptable scalability in most typical hub-and-spoke deployments Scalability becomes challenging for a very large, fully meshed IPSec VPN deployment; may require supplemental planning and coordination to address key distribution, key management, and peering configuration	Not applicable; service provider network is unaware of SSL traffic
Management Site-to-site support	Yes	Yes	No
Remote access support	Yes, if used in conjunction with IPSec	Yes	Yes
Provisioning	Requires one-time provisioning of customer edge and provider edge devices to enable the site to become a member of a MPLS VPN group	Reduces operational expense through centralized network-level provisioning for CPE-based service offering Uses centralized provisioning for network-based service offering	Not applicable; service provider network is unaware of SSL traffic
Service deployment	Needs MPLS-enabled network elements at the core and edge of the service provider network	Can be deployed across any existing IP networks or the Internet	Not applicable; service provider network is unaware of SSL traffic
VPN client	Is not required because MPLS VPN is a network-based VPN service; users do not need VPN clients to interact with the network	Is required for client-initiated IPSec VPN deployments Cisco VPN client software is supported by Microsoft Windows, Solaris, Linux, and Macintosh operating systems	Is not required; relies on Web browser
Place in network	Core network	Local loop, edge, and off-net	Local loop, edge, and off-net
Transparency	Resides at the network layer Transparent to applications	Resides at the network layer Transparent to applications	Works only with applications coded for SSL

Email is another matter. Although It too can be handled with VPN or SMIME where a secure connection is made between client and server, an easier method

uses Pretty Good Privacy (PGP). This uses the secure encryption method developed by Zimmerman to asymmetrically encrypt each email with a private key that can then be un-encrypted with a public key kept at one or more of several key servers around the world. It is non-proprietary and open-source.

As for webpage and web applications, the answer here is SSL over port 443 that provides the familiar https:// and lock in the status bar. If performed at a high enough encryption level, 128k bits or higher, the data is highly protected. As opposed to the asymmetric encryption of public/private keying, with SSL the server hands each new client a key that the client can use to un-encrypt the received data and to encrypt sent data.

For FTP file transfer, SFTP provides the same encrypted secure file transfer that SSL does for web pages and applications. Finally SSH is the secure encrypted form of Telnet that runs over port 22 instead of 23.

Use of the above protocols and algorithms, if implemented correctly will assure the CE that all transmitted EPHI will be safe from prying eyes. With today's technology, you can do almost anything through an encrypted protocol that you can do the with the un-encrypted protocols.

Assignment Three: Policy

EPHI Transmission Encryption Security Policy

1.0 Overview
Implementing Transmission Security Mechanisms are required by the HIPAA Security Rule Standard § 164.312(e)(1) that require security measures to guard against unauthorized assess to as well as certifying integrity of electronic patient health information that is transmitted over electronic communications networks.

2.0 Purpose
The purpose of this policy is to insure the integrity of EPHI as well as prevent unauthorized access to data that is transmitted over electronic communications networks. It establishes procedures that provide the technical means to protect EPHI as it is being transmitted.

3.0 Scope
The scope of the policy will cover EPHI transmitted within the GIAC Health Care Center as well as outside across phone/data lines and the Internet.

4.0 Policy
All Electronic Patient Health Information being transmitted over electronic communication networks must be protected from unauthorized access as well as certifying it's integrity.

4.1 Internal Transmission
All EPHI data within GIAC Health's facility will be transmitted over wired Ethernet lines across switches to prevent broadcasting of data. No wireless connections or access points are permitted on the grounds.

4.2 External Transmission
All EPHI data outside GIAC Health's facility across phone, data, or Internet lines must be encrypted using either 168-bit 3DES or 192-bit AES or 128-bit SSL. Any email going outside the facility must be encrypted with PGP with a key-size greater than 1024-bit. Any files transferred via FTP must use 128-bit SFTP. Any console access of EPHI granted to outside parties must use either SSH or VPN for establishing a connection.

5.0 Enforcement
All employees and contractors of GIAC Health Center are expected to comply with these policies. Network administrators are expected to deploy the appropriate technologies to clients, servers, and network devices to enable the secure transmission of EPHI.

Assignment Four: Procedures

Preventing wireless devices.
Monthly a network administrator will walk through the facilities with a handheld wireless detection device looking for rogue access points. Any found will be confiscated and turned in to the IT department.

Enable Virtual Private Networking
A VPN server will be configured on the firewalls allowing tunneling from a remote client. VPN clients will be installed on any remote computer needing access.

Enable SSL on web servers
All web servers will be enabled for SSL on port 443 so remote users can access with their browsers over https.

Enable SFTP on file servers
All FTP servers will be enabled for SFTP so authorized remote users can download EPHI through encrypted packets.

Enable PGP for email
PGP clients will be installed on all workstations, both internal and external that will be emailing EPHI.

Summary

This document addresses the requirements of the HIPAA Security Rule Standard § 164.312(e)(1) that require security measures to guard against unauthorized assess to as well as certifying integrity of electronic patient health information that is transmitted over electronic communications networks. By defining the environment, explaining the background, setting the policies and developing the procedures, the standard has been fully addressed.

List of References:

[1] DEPARTMENT OF HEALTH AND HUMAN SERVICES Office of the Secretary 45 CFR Parts 160, 162, and 164

[2] Cisco Systems, **MPLS, IPSec, and SSL Comparison**
January 15, 2003 – http://www.cisco.com