Global Information Assurance Certification Paper

-

GIAC Hospital Medical Center

Applying Technology to Meet Information Safeguards Mandated

By Federal Public Law 104-191

HIPAA

Health Insurance Portability and Accountability Act of 1996

Ron Witt

Submitted 10/15/2003

GIAC Information Security Officer (GISO) Certification

Practical Assignment Version 1.3

Table of Contents

Abstract

Federal Public Law 104-191 HIPAA – Health Insurance Portability and Accountability Act of 1996[1] applies to the GIAC Hospital Medical Center.

This document describes the information technology safeguards that the GIAC Hospital Medical Center must apply to meet HIPAA requirements for healthcare information security.

The following information is listed:

- Description of HIPAA mandates and cost of compliance
- HIPAA EDI – Electronic Data Interchange transaction sets
- HIPAA standard data dictionary
- The three categories of HIPAA safeguards: Administrative, Physical and Technical
- The GIAC Hospital Medical Center medical and business operations are described.
- The GIAC Hospital Medical Center network configuration diagrams are included before and after additional security technology is added to the hospital network.
- Three major areas of risks identified at the GIAC Hospital Medical Center which include:
    - Complete Destruction of Patient Healthcare Information
    - Physical security of facilities, offices, desks personal and laptop computers to maintain the security of patient medical and billing information
    - Illicit access to patient medical information
- HIPAA requirements for Administrative, Physical and Technical Security
- A specific security policy is developed GIAC Hospital Medical Center Security Policy focusing on the risk of unauthorized access to patient healthcare data.

- GIAC Hospital Medical Center Security Procedures under the Security Policy

HIPAA

HIPAA – Health Insurance Portability and Accountability Act – Federal Public Law 104-191 was enacted by President Clinton during 1996. HIPAA was designed to meet four distinct requirements:

- Allow individuals to continue healthcare coverage between jobs
- Restrict access to and insure confidentiality of medical information
- Reduce administrative expense through the use of standard EDI – Electronic Data Interchange – transactions to automate insurance coverage status, billing and a variety of manual office operations.
- Reduce health insurance fraud which amounts to billions of dollars billed by providers for medical procedures never performed.

After several years of review and discussion, compliance with HIPAA regulations are now nationally required starting in April of 2003. Medical records and any other medical information that could identify a patient is protected information is covered by HIPAA. HIPAA defines some 68 security requirements that can be divided into three main categories and must be completed by April 2005.

- Technology that insures confidentiality and controls access and security
- Administration Safeguards planning including auditing, records storage and retrieval
- Physical Security of facilities, offices, desks, personal and laptop computers

The projected cost to the Healthcare industry to meet all of the HIPAA mandates will exceed the money spent to meet Y2K – year 2,000 IT conversion estimated at $164 billion. In addition, the Federal Government can impose civil penalties ranging up to $25,000 per violation of HIPAA Federal requirements. Criminal penalties of up to $250,000 and 10 years in prison can be imposed on individuals and organizations committing major violations.

HIPAA regulations cover Healthcare Insurers, Healthcare payer electronic claim clearing houses and any kind of provider – Hospital, Clinic, doctor office, dental, chiropractic optometrist, pharmacist that submits healthcare claims electronically and maintains records on patient treatment.

As an EDI – Electronic Data Interchange - Electronic Billing systems consultant for a major national healthcare insurer, the author will focus on technical security related to flow of medical and billing information over communication networks.

The author will devise a plan for HIPAA security relying on a defense in depth approach that will be weighted toward eliminating the greatest potential risks that include the following:

- Unauthorized access by employees or ex-employees
- Unauthorized access by hackers, criminals, business rivals and vendors
- Systems not configured to response to security incidents

HIPAA Transaction Sets[8]

As a member of ANSI X12, the author was part of the team that developed the Standard EDI HIPAA transaction sets which include:

- Healthcare claim for payment which is also used for coordination of benefits for patients with multiple insurers
    - Institutional (Hospital) claim for payment ASC X12N: Institutional
    - Professional (Doctor) claim for payment ASC X12N: Professional
    - Dental (Dentist) claim for payment ASC X12N: Dental
    - Pharmacy (Prescription Drug) payment NCPCP standard
- Healthcare payment and Electronic Remittance Advice (for automated account posting of transactions) – ASC X12N 835
- Multiple insurer Coordination of Benefits
- Status of claim for payment ASC X12N 276/277
- Electronic Enrollment of patient into an insured healthcare plan ASC X12N 834
- Electronic Eligibility of patient for health insurance ASC X12 270/271
- Electronic payment of heath insurer premiums ASC X12 820

- Electronic medical referral and authorization of a specialist for patient medical services ASC X12N 278

- Attachments to medical claims which provide treatment and diagnostic information for an insurance company to properly adjudicate the claim and set the proper provider payment amount

HIPAA mandates a standard data dictionary to be used with HIPAA transaction sets. The data dictionary consists of the following healthcare industry codes which include:

- ICD-9 The International classification of diseases, related medical conditions, injuries and other kinds of medical problems

- CPT The medical procedures used by doctors and other healthcare workers to treat diseases and mange injuries

- HCPCS These include other medical services, supplies and any medical equipment used to treat the patient

- NCPDP – The National Council for Prescription Drugs used the pharmacy industry coding to identify any prescription drugs prescribed for the patient

The HIPAA security implementation model relies on IT management to develop a security policy based on analysis of potential risks to security and to meet risk with current cost-effective technology. In drafting HIPAA HHS – The Federal Department of Health and Human Services – focuses on results rather than on specific technology which is changing rapidly. An example might be biometrics such as retina scanning which might be prohibitively expensive today but very affordable in the near future.

While leaving the implementation of security technology to be determined by the covered party, HIPAA divides Security Regulations into three areas which include:

- Administrative safeguards

    - covering workforce rules
    - employee training
    - security policies and incident handling procedures
    - backup, recovery and disaster planning

- Physical Safeguards

    - Office security
    - Physical security of desktop and laptop PCs

    - Medical information media storage security

- Technical Safeguards

    - Network level security methods
    - Procedures and policies
    - Data integrity verification
    - Encryption of electronically transmitted information
    - Auditing and logging for intrusion detection
    - Personnel authentication and authorization

HIPAA mandates patient authorization before medical information can be released to a third party. Patient authorization must include the following elements:

- Patients must see a description of any medical information to be disclosed.

- Persons making use of the medical information must be disclosed to patients.

- Any persons releasing the medical information must be disclosed to patients.

- The reason for the disclosure of medical information must be revealed to the patients.

- The patients must sign an agreement to an expiration date which will invalidate consent for disclosure of medical information.

- The patient must date and sign any medical information disclosure agreements.

- If the agreement is signed by a third party on behalf of the patient that relationship must be documented in the agreement.

Assignment One – Describe GIAC Hospital Medical Center

GIAC Hospital Medical Center is located on the state border between two major metropolitan areas. GIAC Hospital Medical Center has 900 employees and has a new five story building. More than 10 million people live within 60 miles of the hospital location.

Originally the city had a public and a parochial hospital that competed for patients and duplicated most hospital services. Starting in the 1980's the two hospitals started cooperating by coordinating medical services. For example, the public hospital offered obstetrics and the parochial hospital was responsible for pediatrics.

The cooperative arrangement worked well into the 1990's when a growing hospital chain built a new hospital in the area. The new hospital aggressively marketed medical services and the original two hospitals suffered a loss of business and decided to merge and build a new $80 million facility – The GIAC Hospital Medical Center.

GIAC Hospital Medical Center is a 400 bed full service acute care hospital offering the following services:

- Behavioral health
- Cancer care
- Cardiac care
- Diabetes care
- Digestive services
- Emergency Room services
- HIV/AIDS clinic
- Home health services
- Home medical equipment
- Hospice care
- Immunotherapy
- Neuroscience services
- Occupational health services
- Ophthalmology
- Pain management
- Pharmacy
- Radiation oncology
- Rehabilitation
- Sleep disorders
- Sports medicine
- Visiting Nurse Association
- Women's health care services

GIAC Hospital Medical Center Data Center

The GIAC Hospital Medical Center Data Center serves both the hospital's business needs and the specific needs of each medical department. With the construction of the new hospital, a secured data center was built in the basement. Physical security was designed with a man-trap entry with a remote video camera to prevent unauthorized entry. The data center was staffed 7 days by 24 hours and only employees with hospital IDs and vendors accompanied by employees are allowed into the data center.

The data center is tied to an enterprise level UPS which is backed up by a diesel generator. In the event of a power failure the data center will maintain non-stop operations as well as critical departments in the hospital. A new fire suppression system has been installed to protect the data center.

With advances in medical technology the operation of the data center continues to become more complex. A variety of third party vendors supply the specialized software applications for most of the hospital's medical departments. The hospital's networking staff provides the first level of support for these applications but relies on off-site vendors to resolve the technical problems with medical department software.

Infrastructure – Network Cabling, Switches and Routers

With the construction of the new hospital all networking cabling was upgraded to CAT5E in both locations with new Cisco 100MB switches and routers. All desktop computers are running Windows XP professional with 100MB network cards connected to departmental Cisco switches. Departmental switches in the communication closets on each floor of the hospital are connected to a high speed FDDI backbone. The network diagram is illustrated in Appendix A.

The network diagram depicts a router configured as a firewall. While this provides some protection against unauthorized intrusion from the Internet, IT management understands this solution does not provide the protection of the dedicated firewall.

The original design is a Class B IP address range in a flat network made up of interconnected switches. The internal IP address range is from 172.16.0.0 to 172.16.254.254 which will support more than 65,000 devices in the hospital and permit future expansion of the network.

Many networking equipment vendors offer software and hardware tools to monitor network performance. The network administration group uses Cisco Works to monitor network performance which provides the following reports:

- Network fault identification
- Network performance monitoring
- Traffic reports to pin point bottlenecks in the network
- Network management control to make router or switch configuration changes
- Access to troubleshooting error logs to diagnose networking faults

As a flat network without subnets connected by routers the network administrator is finding that Ethernet broadcast traffic is increasingly taking up bandwidth. IT management understands that dividing the network into subnets connected by routers will improve performance and security with the creation of VLANs – Virtual Local Area Networks.

Internet – Wide Area Network Infrastructure

The data center has a dedicated high speed T1 link to the Internet maintained by the hospital Internet Service Provider.

Future remote clinic locations will be linked by a hospital owned fiber optic connection – FDDI - running at a gigabit transfer rate. See Appendix A for a network diagram before increased security has been applied to the network.

Data Center – Systems and Applications

Hospital management is supporting a major security system upgrade because of the security demands imposed by HIPAA with the result that security is a major priority of the IT department.

Currently, the hospital has a total of 47 servers which have been installed by third party vendors to support the specialized computing needs of the hospital medical departments. All of the servers at the data center are backed up nightly with tapes rotating with off-site backups.

A cluster of large servers are configured for user file and print service which provides shared folders for departments and individual private directories for users.

The data center has several WEB servers for both the hospital's Intranet and Internet site. The intranet site provides policy information to hospital employees and the Internet site has the following information:

- Information to the public about hospital services

- A phone directory of hospital departments
- A map of the hospital for new visitors
- Tips on maintaining good health

The hospital has two different email systems, one for internal use within the hospital and an external system and is connected to the Internet for outside mail. Microsoft Exchange is used for external mail and Lotus Notes is used for the internal email system. The Notes email system runs on the IBM AS/400 and has been configured with high security and no Internet access.

Dialup access is limited to a small number of employees which includes network administrative staff and some of the hospital's top management. Currently a Windows 2000 RAS server is used for dialup access with a dial back configuration. IT management wants to install a secure VPN connection to allow remote access through the Internet.

The hospitals main system for billing patient records and email is an IBM AS/400 i-Series 820 configured with multiple partitions into several machines. One of the partitions is used for Lotus Notes which is the hospital secure internal Email system. IBM provides the technical support for the AS/400 operating system and maintains the system at the current release of V5R2. IBM reviews AS/400 security monthly and installs any required security patches and operating system upgrades.

In addition to the AS400, the hospital's IT department has a number of Intel based servers running a variety of applications on Windows 2000, Unix and Red Hat Linux:

- WEB Server under Microsoft Internet Information Server II (IIS)
- Intranet Server under Microsoft Internet Information Server II (IIS)
- Application Server running a variety of applications under Windows 2000
- Database Server running Oracle under Red Hat Linux
- An External Email Server running Microsoft Exchange server
- A Microsoft RAS Server to allow remote dial-in access

The new hospital building was commercially wired for Ethernet as a part of the new construction requirements. The contractor installed CAT5e cable with fiber runs between the closets. The original network equipment includes a mixture of hubs, switches and routers from several different manufacturers. Because of the mix of vendor equipment, implementing better security has been a challenge for the IT department.

Hospital management has allocated money for a major upgrade of the network which will provide the security mandated by HIPAA regulations. The security enhancements proposed include the following:

- An operating system upgrade from Windows 2000 to Windows 2003 on all servers. IT will update all servers with current Microsoft patches and hot fixes on a weekly basis.

- The RAS server will be replaced by a VPN which will allow high speed secure remote access.

- A Checkpoint firewall will replace the router acting as a firewall and will provide better protection against attack from the Internet.

- The hubs on each of the floors in the hospital will be replaced by switches so that VLANS can be configured for added security.

- Symantec Anti-virus Enterprise edition will be installed to remotely schedule nightly virus definition upgrades and scans on all PCs in the hospital.

Hospital Business Operations

The hospital's business operations include the following departments located in the main building and supporting the clinic operation:

- Personnel
- Finance
- Patient Billing
- Patient Accounts Receivables
- Marketing
- Facilities Management and Maintenance
- Administration
- Volunteer Services Management

These business operations departments provide services to all hospital department staff, patients of the hospital and the metropolitan community at large.

The major challenge of the hospital's business operations is to upgrade the billing systems to support the key HIPAA EDI transactions mandated for administrative simplification. Medicare billing has been totally automated for electronic billing using the Federal government standards for more than 10 years.

However, billing to most private commercial insurers continues with claims printed on paper and then mailed to each carrier.

The data center needs to upgrade its systems to the support for the following key HIPAA transactions[8] for electronic billing:

- Institutional (Hospital) claim for payment ASC X12N: Institutional
- Professional (Doctor) claim for payment ASC X12N: Professional
- Pharmacy (Prescription Drug) payment NCPCP standard
- Healthcare payment and Electronic Remittance Advice (for automated account posting of transactions) – ASC X12N 835
- Multiple insurer Coordination of Benefits
- Status of claim for payment ASC X12N 276/277
- Electronic Eligibility of patient for health insurance ASC X12 270/271
- Electronic medical referral and authorization of a specialist for patient medical services ASC X12N 278
- Attachments to medical claims which provide treatment and diagnostic information for an insurance company to properly adjudicate the claim and set the proper provider payment amount

The key actions to keep the hospital running are to delivery medical services, bill medical insurers and patients, and maintain the confidentiality of patient medical information. Patient medical information must be protected at all costs.

Assignment Two – Identify Risks

NIST Guide 800-30[13] is a risk management blueprint for IT management to determine the return on investment in matching security technology to potential security threats. The NIST Guide initiates a planning process based on:

- The probability that potential threat will expose a particular vulnerability
- The amount of damage that a particular vulnerability can inflect on an organization
- How effective are current security safeguards for controlling the risk

The hospital IT department focuses on the following business security risks:

Area of Risk 1 - Complete Destruction of Patient Healthcare Information

Risk Overview

HIPAA mandates require administrative safeguards for the physical security of patient healthcare information which include secure records storage. The greatest risk that hospital management has identified is the complete destruction of patient medical records information.

Risk Relevance and Hospital Consequences

- Permanent destruction of patient healthcare information
    - A fire, water damage or a natural disaster that might destroy the data center
    - A hacker attack or a disgruntled employee destroying healthcare information on servers
    - A hacker or a disaster destroying all backup copies of patient medical information

The greatest risk the Hospital Medical Center is the permanent destruction of patient healthcare information which is central to providing healthcare services and financial operations.

To meet HIPAA requirements for physical security the hospital must have administrative procedures and technology in place to reduce the risk. Destruction of healthcare data can come from a variety of sources including fires, water damage, natural disasters, hackers and human errors. The integrity of patient data can be compromised by employees who make malicious changes that go unnoticed and are backed up.

Risk Mitigation

- The data center must have a dry pipe fire suppression system in place with a separate autonomous power source.
- Building blueprints need to be reviewed for the possibility of flooding if water pipes break.
- Server backup operations need to include daily off site backups that are stored in a secure location.

- A disaster recovery plan needs to be in place with a vendor to provide a hot site in case of an emergency and priority sequence for restoring critical services within the hospital.

Area of Risk 2 - Physical security of facilities, offices, desks personal and laptop computers to maintain the security of patient medical and billing information.

Risk Overview

HIPAA mandates require technology that insures confidentiality and controls access and security. The second greatest risk that hospital management has identified is the physical security of facilities, offices, desks personal and laptop computers to maintain the security of patient medical and billing information.

Risk Relevance and Hospital Consequences

Breaches of physical security can impact the delivery of medical services and medical insurance billing operations.

- Short term loss or unavailability of patient healthcare operations
    - Delay or impaired delivery of healthcare services which may result in liability claims against the hospital for patient injuries.
    - Extended or protracted system downtime when healthcare providers have no access to patient medical records
    - Loss of network equipment – servers, PCs, laptops, routers, switches and firewalls
    - Disruption of data center operations impacting patient services, medical records and billing operations

The Hospital Medical Center requires uninterrupted access to healthcare information to provide medical services. Any disruption of network operations will impact medical services.

Risk Mitigation

To meet HIPAA requirements for the security of patient healthcare information the hospital must have administrative procedures and technology in place to reduce the risk.

- Every non-employee who enters the Hospital Medical Center's operation offices has to be identified and monitored. Each employee has an identification badge which they must use to swipe locked doors in secure areas. Only authorized employees are allowed in secure areas. The data center is under constant surveillance with recording video cameras. Like the security in banks tapes can be played back to identify any intruders. Employees must escort non-employees and contractors who enter operations areas.

- Besides the data center all telecommunication closets need to have secure access and there should be nothing on the door to identity the use of these rooms. Like the data center recording video surveillance needs to be in place in the networking and telecommunications closets in the building.

- All employees must attend scheduled classes on hospital security policies and procedures

- As part of security training employees are directed not allowed to take any patient information outside the hospital without management approval.

Area of Risk 3 - Illicit access to patient medical information

Risk Overview

HIPAA mandates require administrative safeguards which include technology that insures confidentiality and controls access and security. The third greatest risk that hospital management has identified is illicit access to patient medical information.

Risk Relevance and Hospital Consequences

In the event of major security violations hospital patients will mistrust the facility and take their business to another medical center. Serious security violations can potentially result in a substantial loss of business with a significant loss of hospital revenue.

- Unauthorized access to patient healthcare information
    - Violation of HIPAA security regulations
    - Potential Federal civil and criminal penalties
    - Loss of business due to customer distrust

- Compromised patient medical information may result in incorrect medical treatment putting the patient at risk and resulting in a liability claim on the hospital.

Risk Mitigation

To meet HIPAA requirements for technical security the hospital must have administrative policies and technology in place to reduce the risk.

- Ongoing employee security training programs have to be regularly scheduled so that employees understand the policies and procedures the Hospital Medical Center has in place to meet HIPAA regulations for healthcare information security.

- HIPAA regulations limit the access to healthcare to employees of the Hospital Medical Center for billing, medical records and office operations. This means that other employees or patients should not be able to view the information on PC monitors or any printed medical records that are sitting on desks.

- The hospital IT department must give network security the highest project priority and conduct regular security audits and reviews.

- Network hubs will be replaced by more secure network switches.

- Firewalls will be added to the network to reduce the risk out outside network intrusions.

- Encryption will be used when electronically transmitting patient information

- IDS – Intrusion Detection Systems will be used to mitigate unauthorized access to the network.

Assignment Three – Evaluate and Develop Security Policies

Evaluation of SANS 'Information Security Policy" Template Related to HIPAA Mandates

SANS developed an "Information Security Policy" template (see Appendix B) to assist companies in the development of corporate security policy. The template serves as an excellent guide for most corporations and relates to information stored in any means and many issues such as not leaving information unattended.

Unlike the SANS guidelines which may not have substantial impact on daily activities in most organizations, HIPAA guidelines are forcing healthcare

organizations to change long standing business operations to meet Federal HIPAA security requirements.

The SANS policy divides company information into three categories: public, more sensitive and the most sensitive business information. The Federal requirements for HIPAA greatly exceed the SANS guidelines for handling even the most sensitive company information.

Under HIPAA guidelines patient medical information can never be given freely to anyone. The following topics compare the SANS most sensitive information to HIPAA requirements.

Access:

SANS: Only those individuals (<Company Name> employees and non-employees) designated with approved access and signed non-disclosure agreements.

HIPAA: Only those individuals who are hospital employees and have approved access for hospital business and medical operations.

Distribution within organization:

SANS: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

HIPAA: All medical information must be handled in a confidential manner and all electronic transmission must be encrypted.

Distribution outside of organization:

SANS: Internal mail: Delivered direct; signature required; approved private carriers.

HIPAA: A patient signed release of information must be obtained before patient information can be sent outside the hospital in a confidential manner.

Electronic distribution:

SANS: No restrictions to approved recipients within <Company Name>, but it is highly recommended that all information be strongly encrypted.

HIPAA: Federal mandates require that all electronic transmission of information must be encrypted.

Storage:

SANS: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

HIPAA: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction:

SANS: Strongly Encouraged: In specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

HIPAA: In specially marked disposal bins on hospital premises for document shredding; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclose:

SANS: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

HIPAA: Up to and including termination, possible Federal civil and/or criminal prosecution to the full extent of the law which may include fines up to $250,000 and ten years in prison.

The previous points illustrate that a HIPAA Information Security Policy needs to be more restrictive than the SANS Information Security Policy. For these reasons the author will develop a security policy based on the SANS template that meet the HIPAA security mandates.

Revised Security Policy to Meet HIPAA Security Mandates

In this section the author develops a specific information security policy for the GIAC Medical Hospital Center to meet the Federal HIPAA mandates for security.

1.0 Purpose

The GIAC Hospital Medical Center security policy is based on the SANS Information Security Template listed in Appendix B. The purpose is to

familiarize employees of their responsibilities to meet HIPAA security guidelines in their handling of healthcare information in the medical facility.

2.0 Scope

Every employee of the Hospital Medical Center must meet HIPAA regulations in the following three areas:

- Administration Safeguards planning including auditing, records storage and retrieval
- Physical Security of facilities, offices, desks, personal and laptop computers
- Technology that insures confidentiality and controls access and security

Regarding confidential patient medical information employees need to exercise good judgment. HIPAA mandates stringent safeguards all employees must follow in controlling access and maintaining the confidentiality of healthcare information. The HIPAA safeguards apply to all employees and violations of GIAC Hospital security policy can result in disciplinary actions including dismissal as well as Federal civil and criminal penalties.

3.0 Policy Statement

HIPAA has put Patient Healthcare information in the most sensitive category of confidential information and relates to: access, distribution with the GIAC Hospital Medical Center, distribution outside the GIAC Hospital Medical Center, Electronic distribution, storage, and disposal/destruction.

Federal Government information security safeguards mandates by Federal Public Law 104-191 HIPAA – Health Insurance Portability and Accountability Act of 1996 apply to the GIAC Hospital Medical Center. All employees are required to adhere to HIPAA security requirements.

3.1 All employees must treat healthcare information as most sensitive confidential

Access: Only those individuals who are hospital employees and have approved access for hospital business and medical operations.

Distribution within organization: All medical information must be handled in a confidential manner and all electronic transmission must be encrypted.

Distribution outside of organization:

A patient signed release of information must be obtained before patient information can be sent outside the hospital in a confidential manner.

Electronic distribution:

Federal mandates require that all electronic transmission of information must be encrypted.

Storage:

Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate

Disposal/Destruction:

In specially marked disposal bins on hospital premises for document shredding; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

3.2 Actions

Actions to Meet HIPAA Administrative Requirements for Security

- Conduct quarterly audit procedure to determine which servers and networking components meet HIPAA security requirements.
- Annually test the disaster recovery, emergency operations and data backup plan for HIPAA compliance.
- Adhere to operating system access control procedure for different levels of employee access to healthcare information.
- Maintain records on levels of employee access and periodically review appropriateness of levels of access quarterly.
- Report HIPAA security violations and incident responses according to chief security officer under reporting plan.
- Security officer has overall responsibility for HIPAA security and risk-assessment and apply cost-effective security solutions.

- Security officer has responsibility for employee violation sanctions and corrective action plans.

- Attend on-going training program for security so that all employees understand HIPAA security requirements for all levels of employee access.

Actions to Meet HIPAA Physical Requirements for Security

- Security officer has overall management responsibility for information and physical security and will be held accountable security procedures, technologies and personnel compliance.

- Follow security officer directives for tracking and controlling access to all Healthcare information and physical security of computers and medical records.

- Follow security officer directives for healthcare information that must be stored in secure facilities with controlled employee access.

- Follow security officer directives for PC and laptop security to limited viewing of healthcare information only to authorized employees. This procedure may require moving PCs in the office.

- Paper copies of patient medical information must be disposed of in bins for shredding and secure disposal.

Actions to Meet HIPAA Requirements for Technical Security

- Examine event logging and reporting on servers continuously to identify unauthorized intrusion of systems. Because of the volume of information the process of log monitoring must be automated with scripts to page IT personnel about suspected intrusions.

- Grant only the least access of operating system or application level access required by an employee to complete their work.

- Use encrypted message authentication, digital signatures, checksums and other technology for email and the transmission of patient medical or billing information.

- Use technology in place to authenticate users with secure user accounts and passwords, biometric technologies, smart cards, and strong authentication methods.

4.0 Enforcement

Employees found in significant and willful violation of the security policies set forward in this document may be subject to:

- Disciplinary action up to and including dismissal
- Potential Federal prosecution with civil finds of up to $25,000
- For major corporate violations Federal prosecution with civil finds up to $250,000 including 10 years in prison

5.0 Definitions

Terms and Definitions

Appropriate measures
To minimize risk to <Company Name> from an outside business connection. <Company Name> computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access <Company Name> corporate information, the amount of information at risk is minimized.

Configuration of <Company Name>-to-other business connections
Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required
Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods
Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential
You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail
Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here…]. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files
Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within

<Company Name> is done via a license. Please contact the appropriate support organization if you require a license.

Company Information System Resources
Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge
To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls
Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use man chmod to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.
Insecure Internet Links
Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of <Company Name>.

Encryption
Secure <Company Name> Sensitive information in accordance with the Acceptable Encryption Policy. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication
One Time Password Authentication on Internet connections is accomplished by using a one time password token to connect to <Company Name>'s internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security
Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for

the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link
A Private Link is an electronic communications path that <Company Name> has control over it's entire distance. For example, all <Company Name> networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employee's homes is a private link. <Company Name> also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which <Company Name> has established private links include all announced acquisitions and some short-term temporary links

6.0 Revision History

Assignment Four – Develop Security Procedures

Security procedures are presented here to address HIPAA security Risk 3 which is stated to prevent unauthorized access to any patient medical information.

The original design of TCP/IP did not anticipate the tremendous growth of the Internet and consequently security was not built into the original specification for IP. Currently, there are a variety of tools that add security to TCP/IP. In the network diagram shown in Appendix C, vendor tools have been applied to increase network security.

Tools and techniques that provide mitigation against packet sniffer attacks on networks

Networks are vulnerable to packet sniffer software which sends all packets passing through a network card to an application that can display text. User names and passwords as well as a number of applications on the network can send in display text: Telnet, FTP, SMTP and POP3.

- By installing switches and removing hubs there will be point to point connections of devices on the network. This is commonly referred to as micro-segmentation. When all devices are connected to switches, sniffers will only capture the information between two devices.

- By encrypting communication on the network, sniffers detecting packets flowing across the network will not be able to read the coded information.

- By installing anti-sniffing tools on the network, administrators can detect the presence of sniffers on the network.

Tools and techniques that provide mitigation against IP Spoofing attacks on networks

Networks are vulnerable to IP Spoofing where hackers use trusted IP addresses and impersonate a trusted user on the network.

- By configuring firewalls to deny traffic coming from outside the network with addresses internal to the network.

- By configuring firewalls to filter traffic

- By host to host authentication

Tools and techniques that provide mitigation against Denial of Service attacks on networks

Networks are vulnerable to Denial of Service - DoS - attacks which focus not on gaining access but rather on making services unavailable. For example, TCP SYN floods can shut down access to Internet WEB sites by consuming all available bandwidth. Another example of DoS is crashing vulnerable daemons which are service providers within the operating system.

- Having the ISP limited the amount of non-essential traffic such as ICMP packets entering the network
- Configuring anti-DoS features on routers and firewalls such as a limit to partially open connections
- Keeping the operating system updated with patches from the vendor

Tools and techniques that provide mitigation against password attacks on networks

Networks are vulnerable to password attacks such as brute force attacks which try different account and password combinations until obtaining a successful logon. Password security can be greatly increased by:

- Encrypted authentication instead of plain text
- 8 character of longer passwords with embedded numbers and special characters
- Different user accounts and passwords for every system users access
- Protection of the password files

Tools and techniques that provide mitigation against Man in the middle attacks on networks

Networks are vulnerable to the Man in the middle attack in which a hacker can hijack a session and gain access to restricted information. These attacks can be prevented by the use of cryptography where all transmitted is encrypted.

Networks are vulnerable to attacks at different layers of the OSI model where hackers exploit weaknesses in the operating system to gain privilege account access. Application layer attacks can be prevented by:

- Use of IDS – Intrusion Detection Systems

- Keeping the operating system current with all service packs, security patches and special vendor fixes
- Disable all un-needed and un-used services
- By using automated tools to monitor system logs to look for patterns of intrusion and issue alarms when intrusion is suspected.

The following security technologies and procedures are applied to the network as represented in Appendix C:

- IDS – Intrusion Detection System provides detection against
    - Application layer attacks
    - Packet sniffers
    - Reconnaissance of the network
    - Port redirection
    - Password brute force attacks over the network
- Switches replacing hubs on each of the hospital floors
    - VLANS – Virtual Local Area Networks
    - Micro-segmentation with only point to point access which stops sniffers from obtaining much useful information
- Firewalls
    - Protects from unauthorized access from the Internet
    - Protects from DoS – Denial of Service attacks

  Edge Router
    - Prevents IP spoofing from the outside
    - Prevents DOS – Denial of Service attacks

  Virus Scanner
    - Prevents virus attacks from known viruses

- Prevents Trojan horse attacks from known Trojans.

VPN Concentrator

- Allows authentication of remote users
- Creates and terminates IPSec tunnels

References

1. Center for Medicare & Medical Services (CMS) Information Systems Security Policy, Standards and Guidelines Handbook Version 1.0, Version 1.0, Department of Health and Human Services, February 19, 2002.

2. "Fact Sheet 8a: HIPAA Basics Medical Privacy", Privacy Rights Clearinghouse, San Diego CA., April 2003.

3. David C. Kibbe, MD, MBA, "A Problem Orientated Approach to HIPAA Security Standards", Family Practice Management July/August 2001, p37.

4. Workgroup for Electronic Data Interchange has information on EDI for healthcare electronic transactions URL: http://www.wedi.org

5. Centers for Medicare & Medicaid Services (CMS) implements HIPAA requirements URL: http://cms.hhs.gov/hipaa/

6. The American Dental Association HIPAA information on EDI for dental practices URL: http://www.ada.org/prof/resources/topics/hipaa/benefits.asp

7. Department of Health and Human Services Web administrative simplifications and cost savings of EDI transactions URL: **http://aspe.os.dhhs.gov/admnsimp/**

8. Washington Publishing Company (WPC) distributes Electronic Data Interchange (EDI) documentation on EDI standards URL: **http://www.wpc-edi.com/hipaa/HIPAA_40.asp**

9. The National Committee on Vital and Health Statistics advises the Secretary of Health and Human Services URL: **http://ncvhs.hhs.gov/**

10. Federal legislative information maintained by the Library of Congress URL: http://thomas.loc.gov

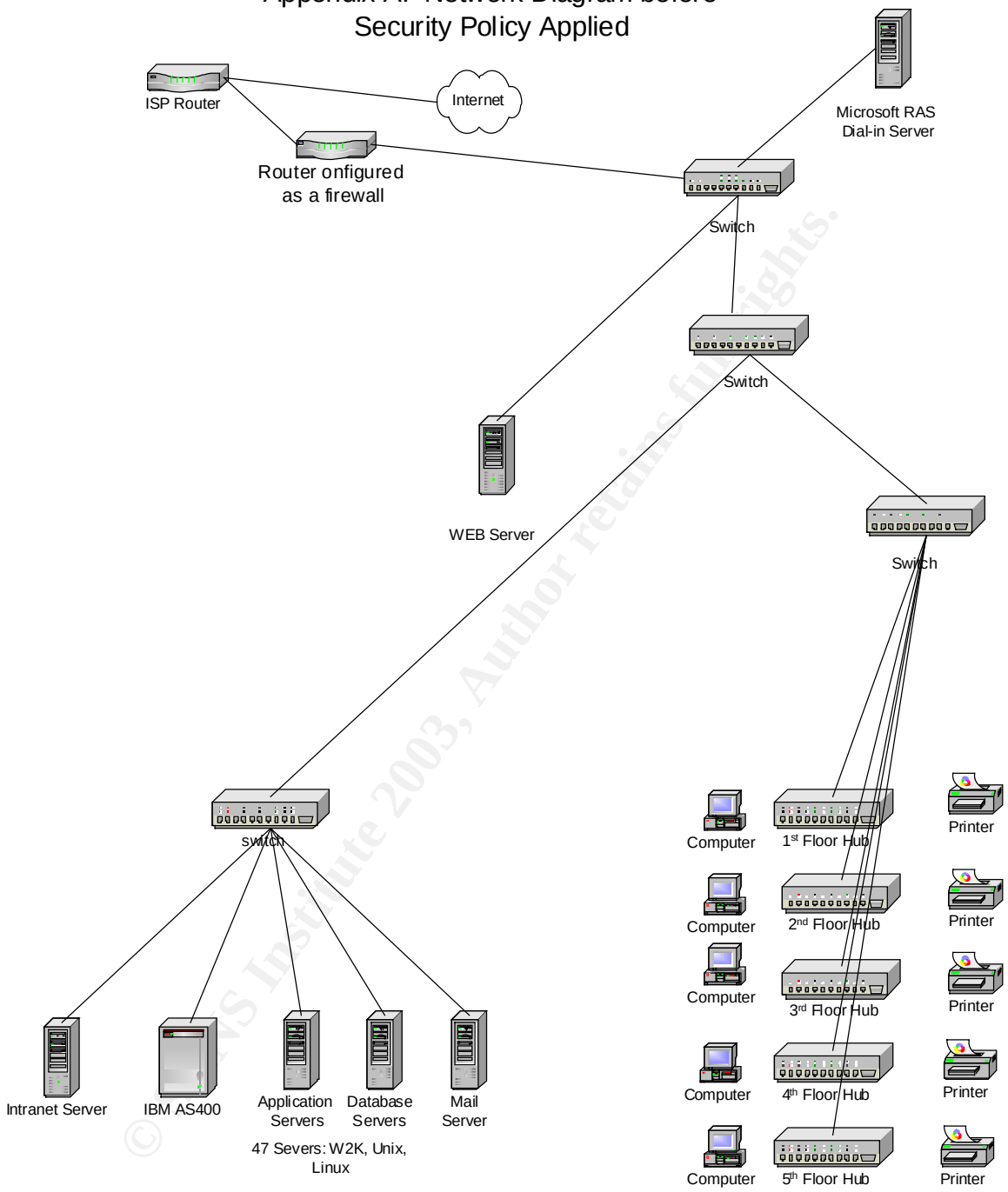
11. The National Council for Prescription Drug Programs, Inc. (NCPDP) is an ANSI-Accredited Standards Development Organization representing the pharmacy services industry URL: http://www.ncpdp.org/main_frame.htm

12. The Health and Human Services - HHS Data Council responsible for coordinating data collection and analysis for the Department of Health

and Human Services, URL: http://aspe.os.dhhs.gov/datacncl/index.shtml

13. Stoneburner, Gary, Goguen, Alice and Feringa, Alexis, "Risk Management Guide For Information Technology Systems", , NIST Special Publication 800-30, National Institute of Standards (February 2002), URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Appendix A: Network Diagram before Security Policy Applied



Appendix B

Information Sensitivity Policy

1.0 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of <Company Name> without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect <Company Name> Confidential information (e.g., <Company Name> Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Infosec.

2.0 Scope

All <Company Name> information is categorized into two main classifications:

- <Company Name> Public
- <Company Name> Confidential

<Company Name> Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to <Company Name> Systems, Inc.

<Company Name> Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in <Company Name> Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of <Company Name> Confidential information is "<Company Name> Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to <Company Name> by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into <Company Name>'s network to support our operations.

<Company Name> personnel are encouraged to use common sense judgment in securing <Company Name> Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

3.0 Policy
The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as <Company Name> Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the <Company Name> Confidential information in question.

3.1Minimal Sensitivity: General corporate information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "<Company Name> Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "<Company Name> Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, <Company Name> information is presumed to be "<Company Name> Confidential" unless expressly determined to be <Company Name> Public information by a <Company Name> employee with authority to do so.

Access: <Company Name> employees, contractors, people with a business need to know.
Distribution within <Company Name>: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of <Company Name> internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
Electronic distribution: No restrictions except that it be sent to only approved recipients.
Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

More Sensitive: Business, financial, technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "<Company Name> Confidential" or "<Company Name> Proprietary", wish to label the information "<Company Name> Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: <Company Name> employees and non-employees with signed non-disclosure agreements who have a business need to know.
Distribution within <Company Name>: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of <Company Name> internal mail: Sent via U.S. mail or approved private carriers.
Electronic distribution: No restrictions to approved recipients within <Company Name>, but should be encrypted or sent via a private link to approved recipients outside of <Company Name> premises.
Storage: Individual access controls are highly recommended for electronic information.
Disposal/Destruction: In specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.1 Most Sensitive: Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that <Company Name> Confidential information is very sensitive, you may should label the information "<Company Name> Internal: Registered and Restricted", "<Company Name> Eyes Only", "<Company Name> Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of <Company Name> Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (<Company Name> employees and non-employees) designated with approved access and signed non-disclosure agreements.
Distribution within <Company Name>: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
Distribution outside of <Company Name> internal mail: Delivered direct; signature required; approved private carriers.
Electronic distribution: No restrictions to approved recipients within <Company Name>, but it is highly recommended that all information be strongly encrypted.
Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions
Terms and Definitions

Appropriate measures
To minimize risk to <Company Name> from an outside business connection. <Company Name> computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access <Company Name> corporate information, the amount of information at risk is minimized.

Configuration of <Company Name>-to-other business connections
Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required
Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods
Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential
You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail
Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here…]. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files
Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within <Company Name> is done via a license. Please contact the appropriate support organization if you require a license.

Company Information System Resources
Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge
To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls
Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use man chmod to find out more about it). On Mac’s and PC's, this includes using passwords on screensavers, such as Disklock.
Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of <Company Name>.

Encryption
Secure <Company Name> Sensitive information in accordance with the Acceptable Encryption Policy. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication
One Time Password Authentication on Internet connections is accomplished by using a one time password token to connect to <Company Name>'s internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security
Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link
A Private Link is an electronic communications path that <Company Name> has control over it's entire distance. For example, all <Company Name> networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employee's homes is a private link. <Company Name> also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which <Company Name> has established private links include all announced acquisitions and some short-term temporary links

Appendix C: Network Diagram after Security Policy Applied