Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Case Study in Implementing Security for HIPAA Privacy Compliance

The Health Insurance Portability and Accountability Act of 1996, otherwise known as HIPAA, set forth new standards for the privacy and security of protected health information (PHI). The timeline set for implementation of the privacy standards was April 14, 2003; however, the security regulations were only in proposed form. It was clear that some security must be in place in order to protect the privacy of PHI. We decided that our greatest area of risk was for unauthorized use and disclosure of PHI, and would therefore...

Copyright SANS Institute

Author Retains Full Rights

AD

Case Study in Implementing Security for HIPAA Privacy Compliance

Ellen Robinson
June 21, 2003
GSEC Practical
Assignment Version 1.4b
Option 2

Abstract

The Health Insurance Portability and Accountability Act of 1996, otherwise known as HIPAA, set forth new standards for the privacy and security of protected health information (PHI). Once the Y2K crisis had come and gone, healthcare organizations could now turn their attention to these new regulations. Interpretation of the regulations proved to be a daunting task. The timeline was set for implementation of the privacy standards for April 14, 2003; however, the security regulations were only in proposed form. It was clear that some security must be in place in order to protect the privacy of PHI. We decided that our greatest area of risk was for unauthorized use and disclosure of PHI, and would therefore focus on protecting the confidentiality of PHI.

The approach that was taken was to identify the security standards from the proposed rule that addressed confidentiality, as opposed to availability and integrity. Plans were developed and responsibilities assigned to focus on the security standards chosen. The final security regulations were published February 20, 2003, and an analysis was done to see how our selection of standards from the proposed rule measured up against the final rule. Our assessment is that we chose wisely, which put us in an excellent position for both privacy and security compliance. Many believe that the final security regulations are what will be used to measure against today in the event of a privacy breach, even though the compliance date for security isn't until April 20, 2005. Today we have a sound security program in place, which will enable us to meet and probably exceed the requirements set forth in the final rule well before the 2005 compliance date.

In the Beginning…

The "Standards for Privacy of Individually Identifiable Health Information" Federal Register 160.102, as part of Health Insurance Portability and Accountability Act of 1996 (HIPAA), was effective 04/15/2003. The regulations contain standards that require health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form with a transaction covered in the rule, to protect patients' rights regarding their health information. The standard for "Safeguards" includes what is commonly referred to as the "mini security rule". This rule states:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

§ 164.530 Administrative requirements.
c)(1) *Standard: Safeguards*. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.
2) *Implementation specification: Safeguards.*
A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(Federal Register Part II Department of Health and Human Services Office of the Secretary 45 CFR Parts 160 and 164. "Standards for Privacy of Individually Identifiable Health Information; Final Rule")

While specific implementation requirements are not stated in this standard, it is implied that the final security regulations will meet this requirement.

"In the context of HIPAA, there is no privacy without security. The HIPAA Privacy Regulation mandates that security safeguards be in place to protect privacy," A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."[2] Healthcare organizations' efforts in implementing the HIPAA Security Standards will affect their ability to comply with the HIPAA Privacy regulations." It should be noted that the implementation of reasonable and appropriate security measures also supports compliance with the privacy standards, just as the lack of adequate security can increase the risk of violation of the privacy standards."[3]

1 HIPAA Security Standards: Preamble (45 CFR Parts 160, 162, and 164)
2 HIPAA Standards for Privacy of Individually Identifiable Health Information (45 CFR Parts 160 and 164)
3 HIPAA Security Standards: Preamble (45 CFR Parts 160, 162, and 164)

(RSA Security. "No Privacy Without Security: The HIPAA Privacy Regulation's Requirement for Security")

The published Security and Electronic Signature Standards; Proposed Rule (otherwise referred to NPRM for Notice of Proposed Rulemaking) contained the only available specific security standards to consider for privacy compliance. This, in combination with other best practices, primarily ISO 17799, is what we chose for guidance for the security implementation requirements. It was not known how it might be judged as to what security is deemed appropriate and reasonable, or within what timeframe it would be expected. The level and areas of risk needed to be assessed, and a documented approach with written justification was required in the event a complaint or lawsuit.

The Department of Health and Human Services (DHHS) will impose fines to organizations for non-compliance, however, the greater liability in the event of a

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

breach, would be from civil suits, and the resulting monetary loss and reputation damage.

It is well known that all three of the tenets of security (confidentiality, integrity, and availability) are important for a sound security program, however, for reducing the risk of an unauthorized use or disclosure of PHI, we chose to focus on protecting confidentiality.

While HIPAA is a primary driver for security, there are other security laws and regulations, both at the state, federal, and international level that must be considered in developing an information security program. It was determined that a comprehensive information security program was required, and that HIPAA would be a component of it, with the priority for any implementation requirements to be in line with the specific compliance dates.

One individual was responsible at the time to oversee and create information security governance. With the new regulatory climate and an increasing level of new security threats in an organization heavily reliant on its strategic information assets, it was clear that additional security resources needed to be in place. A new Chief Information Security Officer was hired. Approval was obtained to hire additional resources for Security Policy and Architecture, Security Program Office, IT HIPAA Program Office, and Security Audits. I was hired as the Director of the IT HIPAA Program Office, and was also assigned responsibility for Security Administration.

Our current Information Security Policy needed to be evaluated and updated to ensure compliance with HIPAA and all the various legal and regulatory requirements. It was unclear at the time how much of what was included in the policy was actually in practice. It was agreed that a policy review and revision would be necessary, based on the HIPAA NPRM and best practices in the industry. In addition, there were no standards for security in place for all the technical components to include operating systems, databases, and applications. It was not known what security features were being utilized and where all the vulnerabilities were, since each area of responsibility determined its own security requirements. The focus for most system administrators and developers was on operational concerns and initiatives, not security. Technical standards needed to be established and implemented.

Many technical security controls were already in place:

- A network intrusion detection system to continually monitor Internet, Extranet, and Internal communications
- Network firewalls that require a rigorous firewall change request process
- RSA SecurID time-based token system for strong authentication for employee remote access
- VPN connectivity utilizing 168bit 3DES encrypted IPSec tunnels

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Secure file transfer via the Internet utilizing minimally 168 bit SSL encryption
- Secure email via S/MIME-based encryption technologies and X.509 Digital Certificates
- Virus Protection for all computer workstations and servers

Implementing the Security Solutions:

A review and interpretation of the HIPAA Security Notice of Proposed Rulemaking (NPRM) was needed to understand what security requirements would be needed for HIPAA Privacy compliance. This involved reviewing each standard of the NPRM to determine which ones impacted confidentiality. The standards selected are highlighted in bold in the table below:

Security and Electronic Security Standards Proposed Rule - Addendum 1

HIPAA Security Matrix.

Administrative Procedures To Guard Data Integrity, Confidentiality, and Availability

Requirement	**Implementation**
Certification	
Chain of trust partner agreement	
Contingency plan (all listed implementation features must be implemented).	Applications and data criticality analysis. Data backup plan. Disaster recovery plan. Emergency mode operation plan. Testing and revision.
Formal mechanism for processing records.	
Information access control (all listed implementation features must be implemented).	**Access authorization.** **Access establishment.** **Access modification.**
Internal audit	
Personnel security (all listed implementation features must be implemented).	**Assure supervision of maintenance personnel by authorized, knowledgeable person.** **Maintenance of record of access authorizations.** **Operating, and in some cases, maintenance personnel have proper access authorization.** **Personnel clearance procedure.** **Personnel security policy/procedure.** System users, including maintenance personnel,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

	trained in security.
Security configuration mgmt. (all listed implementation features must be implemented).	Documentation. Hardware/software installation & maintenance review and testing for security features. **Inventory.** Security Testing **Virus checking.**
Security incident procedures (all listed implementation features must be implemented).	**Report procedures.** **Response procedures.**
Security management process (all listed implementation features must be implemented).	**Risk analysis.** **Risk management.** **Sanction policy.** **Security policy.**
Termination procedures (all listed implementation features must be implemented).	**Combination locks changed.** **Removal from access lists.** **Removal of user account(s).** **Turn in keys, token or cards that allow access.**
Training (all listed implementation features must be implemented).	**Awareness training for all personnel (including mgmt).** **Periodic security reminders**. **User education concerning Virus protection.** **User education in importance of monitoring log in success/failure, and how to report discrepancies.** **User education in password management.**

Physical Safeguards To Guard Data Integrity, Confidentiality, and Availability

Requirement	**Implementation**
Assigned security responsibility	
Media controls (all listed implementation features must be implemented).	**Access control.** **Accountability (tracking mechanism).** Data backup. Data storage. **Disposal.**
Physical access controls (limited access) (all listed implementation features must be implemented).	Disaster recovery. Emergency mode operation. **Equipment control (into and out of site).** **Facility security plan.** **Procedures for verifying access authorizations prior to physical access.** Maintenance records. **Need-to-know procedures for personnel access.** **Sign-in for visitors and escort, if appropriate.** Testing and revision.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Policy/guideline on work station use	
Secure work station location	
Security awareness training	

Technical Security Services To Guard Data Integrity, Confidentiality, and Availability

Requirement	Implementation
Access control (The following implementation feature must be implemented: Procedure for emergency access. In addition, at least one of the following three implementation features must be implemented: Context- based access, Roll-based access, User- based access. The use of Encryption is optional).	Context-based access. **Encryption.** **Procedure for emergency access.** **Role-based access.** **User-based access.**
Audit controls	
Authorization Control (At least one of the listed implementation features must be implemented).	**Role-based access.** **User-based access**
Data Authentication	
Entity Authentication (The following implementation features must be implemented: Automatic logoff, Unique user identification. In addition, at least one of the other listed implementation features must be implemented).	**Automatic logoff.** Biometric. **Password.** **PIN.** Telephone callback. **Token.** **Unique user identification.**

Technical Security Mechanisms To Guard Against Unauthorized Access to Data That Is Transmitted Over a Communications Network

Requirement	Implementation
Communications/network controls (The following implementation features must be implemented: Integrity controls, Message authentication. If communications or networking is employed, one of the following implementation features must be implemented: Access controls, Encryption. In addition, if using a network, the following four implementation features must be implemented: Alarm, Audit trail, Entity authentication, Event reporting).	**Access controls.** Alarm. Audit trail. **Encryption.** **Entity authentication.** **Event reporting.** Message authentication. Integrity controls.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Electronic Signature

Requirement	Implementation
Digital signature (If digital signature is employed, the following three implementation features must be implemented: Message integrity, Non-repudiation, User authentication. Other implementation features are optional).	Ability to add attributes. Continuity of signature capability. Counter signatures. Independent verifiability. Interoperability. Message integrity. Multiple Signatures. Non-repudiation. Transportability. User authentication.

(Federal Register Part III Department of Health and Human Services Office of the Secretary 45 CFR Part 142. "Security and Electronic Signature Standards; Proposed Rule".)

This selected standards for the security required for privacy compliance were reviewed and approved by Legal and Compliance. The following items describe the implementation steps identified in the requirements agreed upon above.

Assigned Security Responsibility:
The organization appointed a Data Privacy and Security Officer (DPSO) who reported in through Legal and Compliance. A HIPAA Steering Committee was then established and in addition a HIPAA Oversight Committee that included representation from various segments of the business. The CISO was a member of both these committees, while I was an active member of the HIPAA Oversight Committee.

The CISO then established an Information Technology Security Steering Committee and an Information Security Program Office. The first step was to set up the information security organization and define the roles and responsibilities. A formal Security Charter that defined the security roles and responsibilities was written, with the help of outside consultants. The document was reviewed and updated by the Information Security Steering Committee and submitted to the Executive Business Management for approval.

Security Management Process:
In order to assess what our security vulnerabilities were, we needed to make a comparison to industry best practices. While the HIPAA Security NPRM regulation covered a fairly comprehensive set of standards, it was only in proposed form, and we wanted to know where we stood against a standard that was already in practice. We chose ISO 17799: A Standard for Information Security Management.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

"ISO 17799 is "*a comprehensive set of controls comprising best practices in information security*". It is essentially an internationally recognized generic information security standard.

Its predecessor, BS7799-1, has existed in various forms for a number of years, although the standard only really gained widespread recognition following publication by the International Standards Organization (ISO) in December 2000. Formal certification and accreditation were also introduced around the same time.

The standard comprises ten prime sections:

- *Business Continuity Planning*
- *System Access Control*
- *System Development and Maintenance*
- *Physical and Environmental Security*
- *Compliance*
- *Personnel Security*
- *Security Organization*
- *Computer & Operations Management*
- *Asset Classification and Control*
- *Security Policy*

Within these are the detailed statements that comprise the standard."

(ISO17799 Information Security Group, "The ISO 17799 Directory")

As we examined the detail contained within the ISO 17799 standard, we saw that the standards in the NPRM were addressed within the ISO 17799 standard. By following the ISO 17799 standard as a framework, we were comfortable that we would be implementing a security program that would meet or exceed HIPAA's requirements.

Risk Analysis:
A security risk assessment was accomplished by reviewing a representative sampling of the entire corporation's personnel, IT assets, and physical locations, and entailed a number of separate components to provide an overall, detailed picture of the security posture. The components consisted of:

- A detailed security policy and procedures analysis in the context of the ISO 17799 Information Security Management Standard and the Health Insurance Portability and Accountability Act (HIPAA) proposed security rule, and identification of any existing gaps
- Interviews with key personnel from the organization
- Open Source Intelligence (OSI) that examines the image of the organization in the Internet community

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Penetration testing to assess the current level of technical security

The resulting document produced a list of all findings for security vulnerabilities, and then prioritized them into risk categories, with recommendations for remediation. The priority denoted a severity or impact to the business based on the duration of time to correct. The categories were as follows:

- Very High Risk – Systemic or major program issues and regulatory violations that pose significant compliance or security risk

- High Risks – The most critical issues, posing an immediate danger to business due to gaps in the security of the network and connected systems/hosts. These should be addressed immediately.

- Medium Risks – The issues that should be addressed in a timely manner, but do not pose substantial immediate risk to the organization

- Low Risks – The issues that should be noted and implemented from these gaps is moderate and can be addressed in the normal course of business.

While this risk assessment proved to be very valuable, we realized that this needed to be an ongoing process. A recommendation was made for a vulnerability assessment tool, which was submitted and approved for purchase during the budget cycle. Penetration tests would be performed periodically to provide additional information.

Interestingly, all of the findings that needed to be addressed from the higher risk categories were around protecting confidentiality. This worked well for our plan to address the confidentiality requirements as a priority.

<u>Risk Management:</u>
The Information Security Program Office adopted a risk management program that included following:

- Security evaluations utilizing intrusion detection, penetration tests, and a multi-tiered virus defense
- Threat monitoring utilizing security vulnerability subscription lists
- Computer Incident Response Plan
- Security review throughout project life-cycle
- Security benchmarking utilizing consultants, research, and conference attendance
- Referencing industry standards, i.e. ISO 17799, NIST
- Risk evaluation for new applications and software products
- Internal and external audits

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Sanction Policy:
A Sanction Policy was developed by the Data Privacy and Security Officer in conjunction with Human Resources and published. The policy included sanctions for both privacy and security violations. This was communicated to all employees through the annual Compliance Training Program and is provided to all employees at new hire orientation.

Security Policy:
The Information Technology Security Steering Committee was tasked with creating a security policy document. An outside consultant was retained to provide written policies based on the ISO 17799 information Security Standard. The Committee then reviewed the document for modifications and once approved, was sent to leadership representatives from the business, to include Legal and Compliance, Human Resources, and Facility Security. The final step was getting approval and sign-off from the Executive Business Management Team.

Chain of Trust (Business Associate Agreements):
We considered Chain of Trust Agreements as Business Associate Agreements with security language included. The Privacy regulation requires that Business Associates are identified and agreements be in place either by April 14. 2003 where none existed already, or by April 14, 2004 for those that already had agreements in place. The Business Associate Agreement was prepared by Legal and contained language for both privacy and security. All those identified as required by April 14, 2003 were updated and the remaining prioritized for updating based on renewal date to be completed prior to April 14, 2004.

Personnel Security:
The security policy document we developed contained a Personnel section. We extracted the policies that pertained specifically to employees that addressed their security responsibilities. This was published as a separate document and distributed to all employees. It is posted on the intranet and is included in every new hire packet. Human Resources reviewed and approved the policies for personnel clearance. All employees go through a thorough background check and drug testing prior to being hired.

Security Configuration Management:
Inventory:
An inventory was taken for all hardware, operating systems, databases, and applications for all locations. Each component was then identified for where protected health information was stored or processed. The inventory process was manual since there was no automated process or centralized repository in place. Since there was considerable effort required to establish a current inventory, a recommendation was made to purchase a solution going forward to ensure an inventory would be available at any time.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Termination Procedures:
Polices for termination procedures were included in the Information Security Policy document. It outlined the manager's responsibilities for notification and the retrieval of items such as computer equipment, tokens, cell phones, and badges. Departing employees must be observed at all times while they are packing. Any former employees, consultants, or contractors who were terminated for cause should not be rehired or contractually retained. A termination checklist was developed and distributed to all managers to assist them in ensuring all items are completed.

Information Access Control:
Minimum Necessary:
The minimum necessary provision of the HIPAA Privacy regulation does create a need for access controls. Access to electronic PHI through systems must address an individual's access rights to only the minimum necessary information needed to perform their duties.

"The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information."

(OCR HIPAA Privacy, "Minimum Necessary [*45 CFR 164.502(b), 164.514(d)*]")

Roles were defined for the entire organization and a standard access matrix was developed. Managers were required to review their employee's access based on the standard and ensure that access was appropriate based on their job function. Systems were identified that needed remediation to be able to control the access based on the roles and access authorizations defined. Some systems required re-design and plans for remediation were developed. Access that could not be changed prior to the Privacy deadline was documented, and employees were instructed as to their responsibilities in keeping the information confidential.

Security Administration Procedures:
A Security Administration System Access Request Standard Operating Procedure was developed that included the following procedural requirements:

- Enrolling New Users
- Modifying User Access
- Revoking User Access
- Setting up Temporary Access
- Monitoring User Access
- Emergency Access
- Monitoring Login Success/Failure

In addition a Standard was developed for System Access Request Forms.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

As part of the inventory, the names of all people who performed the duties of a security administrator for user accounts were identified for each operating system, database, and application. Training sessions via conference calls were held to review the new procedure. Over 120 security administrators were identified and added to an email group that would receive bi-weekly files from the Human Resources system for new hires, transfers, terminations, and name changes. While policies and procedures were already in place that required managers to report employee transfers, terminations, and name changes, the assessment revealed that this process was not always followed. By using the files from the Human Resource system, the security administrators were now able to keep the access privileges current.

Testing with Production Data:
Testing with confidential PHI production data was sometimes required both internally and with external parties. Access controls and adherence to the minimum necessary standard would need to be implemented to ensure the confidentiality of the data from unauthorized use and disclosure.

We decided that creating a standard was necessary to give guidance on the security controls required when using "live" data. The HIPAA Privacy Standard for the De-Identification of Health Information provides a list of 19 data elements that must be removed if one wants to use the data without having to adhere to any of the privacy and security regulations. Where the de-identification of PHI data was not possible to effectively test, the following standard must be followed:

- Where using PHI is allowed, production data must be de-identified as much as possible, without compromising the quality of testing.
- All copies of PHI data must be destroyed through the clearing of the environment after authorized use is completed.
- All testing environments must comply with all company security standards.
- Security administration procedures must be followed for all testing environments, i.e. strict maintenance of user account privileges.
- All standards for minimum necessary must be followed.
- Testing with external entities is allowed only with other covered entities, unless a valid business associate agreement is place prior to any testing.
- The data used for testing must come from the same population of data that the external entity would normally receive in production runs.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Awareness Training:
The HIPAA Program Office included basic security awareness training as part of the annual Compliance Training Program for privacy. It included:

- Don't share your passwords
- Don't write your password down on paper
- Report any security incidents you become aware of
- Handling suspected viruses

In addition, a security checklist was created for managers to distribute to their employees in a true/false questionnaire format. The security policies were posted on the intranet, and news about it was published in the company newsletter.

Security Incident Procedures:
A Computer Security Incident Response plan was written and tested. Roles and responsibilities were defined for the Computer Security Incident Response Team (CSIRT). They included the following: CSIRT Officer, Alternate CSIRT Officer, CSIRT Manager, Alternate CSIRT Manager, CSIRT Staff, CSIRT Decision Pool and Adjunct CSIRT Decision Pool, CSIRT Response Team, and a CSIRT Recovery Team. General guidelines for primary response services were developed and included in the written plan. These were broken down into the following section: Alert, Triage, Response, Recovery, and Maintenance. A simulated incident was planned and tested to ensure the plan was effective.

Internal Audit:
An outside auditing firm was engaged to assess whether our project plan was acceptable for preparing for the security requirements necessary for privacy compliance. In addition, an audit was scheduled for August 2003 to ensure the security was implemented according to plan. An additional review of our full security plan based on the final regulations would be performed once the final regulations were published and interpreted.

Secure Workstation Location:
All workstations were reviewed to ensure the location was deemed appropriate for minimizing disclosures and relocated where necessary. With our roll-out of Windows 2000 on all workstations, automatic screen timeouts were instituted throughout.

Physical Access Controls:
All locations where PHI was housed were identified. Existing written procedures were reviewed and updated where necessary to include the following:

- physical access entry controls, i.e. key, combination locks, or electronic card reader systems
- identification of individuals authorized to approve access as well as the maintenance of access control lists
- a process for removing access for individuals no longer authorized, i.e. terminated employees

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- steps to follow for emergency access
- requirement for visitor escorts and sign-in logs
- a periodic review of the access logs

Policy/Guideline on Workstation Use:
The Information Security Policy document included various policies to cover the workstation use requirements. A separate employee policy document was published and distributed. In addition, an Access Agreement was developed that outlined the security responsibilities and was required to be signed by each newly hired employee. Temporary help and Contractors are also required to sign the agreement.

Media Controls - Disposal:
HIPAA requires removing PHI data from electronic media before disposing of it. We determined the need for a standard to follow throughout the organization.

"There has been a standard in place for some time that addresses the problem of permanent removal of data from a hard drive. The standard was developed by the Defense Security Service (DSS) and is used by many federal and commercial organizations. Under the National Industrial Security Program (NISP), DSS Industrial Security Representatives oversee cleared contractor facilities and assist the organizations' management staff and Facility Security Officers in formulating their security programs. As part of the NISP initiative, DSS has developed the DOD standard 5220.22-M NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL. Among other items, the standard outlines the method to be used for removing data from unclassified hard drives – sanitizing. NISP defines an overwriting technique that will remove any existing data yet leave the hard drive in a state where it can be reused. The process involves the following two steps:

1. Before any sanitization product is acquired, careful analysis to the overall costs associated with overwrite/sanitization should be made. Depending on the contractor's environment, the size of the drive and the differences in the individual products time to perform the sanitization, destruction of the media might be the preferred (i.e., economical) sanitization method.

2. Overwrite all addressable locations with a character, then its complement. Verify "complement" character was written successfully to all addressable locations, then overwrite all addressable locations with random characters; or verify third overwrite of random characters. Overwrite utility must write/read to "growth" defect list/sectors or disk must be mapped before initial classified use and remapped before sanitization. Difference in the comparison lists must be discussed with the DSS Industrial Security Representative (IS Rep) and/or Information System Security Professional (ISSP) before declassification. ***Note:*** *Overwrite utilities must be authorized by DSS before use.*

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(Hardwick, Steve, "Secure Removal of Protected Health Information: Cleaning Hard Drives to the HIPAA Standard Prior to Disposal or Donation")

We decided to follow the DOD Standard "The National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M" for the clearing and sanitization of all forms of storage media. The standards are as follows:

Department of Defense
Clearing and Sanitization Matrix
(DOS 5220.22-M)

Media	Clear	Sanitize
Magnetic Tape1		
Type I	a or b	a, b, or m
Type II	a or b	b or m
Type III	a or b	m
Magnetic Disk		
Bernoullis	a or c	m
Floppies	a or c	m
Non-Removable Rigid Disk	c	a, d, or m
Removable Rigid Disk	a or c	a, d, or m
Optical Disk		
Read Many, Write Many	c	m
Read Only		m, n
Write Once, Read Many (Worm)		m, n
Memory		
Dynamic Random Access memory (DRAM)	c or g	c, g, or m
Electronically Alterable PROM (EAPROM)	i	j or m
Electronically Erasable PROM (EEPROM)	i	h or m
Erasable Programmable (ROM (EPROM)	k	l, then c, or m
Flash EPROM (FEPROM)	i	c then i, or m
Programmable ROM (PROM)	c	m
Magnetic Bubble Memory	c	a, b, c, or m
Magnetic Core Memory	c	a, b, e, or m
Magnetic Plated Wire	c	c and f, or m
Magnetic Resistive Memory	c	m
Nonvolatile RAM (NOVRAM)	c or g	c, g, or m

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Read Only Memory ROM		m
Static Random Access Memory (SRAM)	c or g	c and f, g, or m
Equipment		
Cathode Ray Tube (CRT)	g	g
Printers		
Impact	g	p then g
Laser	g	o then g

Clearing and Sanitization Matrix

a. Degauss with Type I, II, or III degausser.

b. Degauss with same Type (I, II, or III) degausser.

c. Overwrite all addressable locations with a single character.

d. Overwrite all addressable locations with a character, its complement, then a random character and verify. THIS METHOD IS NOT APPROVED FOR SANITIZING MEDIA THAT CONTAINS TOP SECRET INFORMATION.

e. Overwrite all addressable locations with a character, its complement, then a random character.

f. Each overwrite must reside in memory for a period longer than the classified data resided.

g. Remove all power to include battery power.

h. Overwrite all locations with a random pattern, then with binary zeros, and finally with binary ones.

i. Perform a full chip erase as per manufacturer's data sheets.

j. Perform i above, then c above, a total of three times.

k. Perform an ultraviolet erase according to manufacturer's recommendation.

l. Perform k above, but increase time by a factor of three.

m. Destroy - Disintegrate, incinerate, pulverize, shred, or melt.

n. Destruction required only if classified information is contained.

o. Run one page (font test acceptable) when print cycle not completed (e.g. paper jam or power failure). Dispose of output as unclassified if

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

visual examination does not reveal any classified information.

p. Ribbons must be destroyed. Platens must be cleaned.

q. Inspect and/or test screen surface for evidence of burned-in information. If present, the screen must be destroyed.

NOTE: As of 22 April, 2002 shredding of IA products is not authorized.

(Phoenix Health Systems, HIPAAdvisory.com. "Disk Sanitization")

We were currently using a third party for the disposal of our electronic media, so we updated our contract with the vendor. Since the vendor is considered a business associate under HIPAA, our contract already included the standard privacy and security language required under the law. Additional language was added that the vendor must agree to adhere to our standard and provide a printed certification for accountability attesting to the disposition of media or systems they have been contracted to dispose.

Technical Security Services/Mechanisms:

The compliance status for each inventory component was assessed for the technical requirements for unique user ID/password, automatic logoff, and encryption over the internet. Any areas that were found to be non-compliant were required to either remediate prior to the April 14, 2003 deadline or submit a request for a deviation. The deviation was to include the reason as well as include any plans for remediation or replacement. The deviation requests were then reviewed by the Chief Information Officer, the Chief Information Security Officer, the Data Privacy and Security Officer, Legal, and the HIPAA Steering Committee. All documentation will be kept for a period of 6 years, as required by the regulation, and all remediation and replacement efforts are being tracked as projects until completion.

Since the security configurations for all systems was left to the individual owners of the information assets, it was necessary to define the required security and develop technical standards. All effected systems would have to develop plans to bring their systems up to the standard and all systems would require the standards be in place before any new implementations.

Technical standards were developed for all operating systems, databases, and applications. While the only technical standards required for implementation by April 14, 2003 deadline were for unique user ID/password, automatic logoff, and encryption, written plans for the implementation of the remaining standards were required. Examples of areas included in the technical standards are:

- Server Configuration
- Application Interface Configuration

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Access Control
- Security Administration
- Passwords
- Permissions
- Authentication
- Auditing and Logging

The Security Environment Today:

All projects were completed prior to the April 14, 2003 deadline. The audit that is scheduled for August will give us information regarding the success of our implementation. Since security is an on-going process, we will continue to audit on a regular basis to ensure the required security is in practice. We have documented our project plans, activities and decisions, in the event we ever need to show our due diligence. We now have a program in place with security responsibilities assigned and will continue to review the security vulnerabilities found through audits and incident reporting. Risk management is the foundation in which we will continue to remain on top of any new and existing threats and vulnerabilities identified.

All new projects go through a security review during the initiation phase. New applications are required to be risk scored based on criteria we developed. This ensures that the appropriate security controls are put into place. Our Project Execution Program required a security checklist must be signed-off on before any project can be put into production. Technical standards are defined for all new implementations, with projects in place for all existing systems to re-mediate within projected timelines.

The final HIPAA Security regulation was published Feb 20, 2003. Highlighted in the table below are the requirements that were met through the implementation of security for privacy.

Appendix A to Subpart C of Part 164—Security Standards: Matrix

Standards	Implementation Specifications (R)=Required, (A)=Addressable
164.308(a)(1)Security Management Process	**Risk Analysis (R)**
	Risk Management (R)
	Sanction Policy (R)
	Information System Activity Review (R)
164.308(a)(2 Assigned Security Responsibility	**(R)**
164.308(a)(3)] Workforce Security	**Authorization and/or Supervision (A)**
	Workforce Clearance Procedure (A)
	Termination Procedures (A)
164.308(a)(4) Information Access Management	Isolating Healthcare Clearinghouse Function (R)
	Access Authorization (A)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Standards	Implementation Specifications (R)=Required, (A)=Addressable
	Access Establishment and Modification (A)
164.308(a)(5) Security Awareness and Training	**Security Reminders (A)**
	Protection from Malicious Software (A)
	Log-in Monitoring (A)
	Password Management (A)
164.308(a)(6) Security Incident Procedures	**Response and Reporting (R)**
164.308(a)(7) Contingency Plan	Data Backup Plan (R)
	Disaster Recovery Plan (R)
	Emergency Mode Operation Plan (R)
	Testing and Revision Procedure (A)
	Applications and Data Criticality Analysis (A)
164.308(a)(8 Evaluation	**(R)**
164.308(b)(1 Business Associate Contracts and Other Arrangement.	**Written Contract or Other Arrangement (R)**
164.310(a)(1) Facility Access Controls	Contingency Operations (A)
	Facility Security Plan (A)
	Access Control and Validation Procedures (A)
	Maintenance Records (A)
164.310(b) Workstation Use	**(R)**
164.310(c) Workstation Security	**(R)**
164.310(d)(1 Device and Media Controls	**Disposal (R)**
	Media Re-use (R)
	Accountability (A)
	Data Backup and Storage (A)
164.312(a)(1) Access Control	**Unique User Identification (R)**
	Emergency Access Procedure (R)
	Automatic Logoff (A)
	Encryption and Decryption (A)
164.312(b)] Audit Controls	**(R)**
164.312(c)(1 Integrity	Mechanism to Authenticate Electronic Protected Health Information (A)
164.312(d Person or Entity Authentication	**(R)**
164.312(e)(1) Transmission Security	Integrity Controls (A)
	Encryption (A)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(Federal Register Part II Department of Health and Human Services, Office of the Secretary 45 CFR Parts 160, 162, and 164, "Health Insurance Reform: Security Standards; Final Rule")

As you can see, the majority of items we addressed were included in the privacy implementation. Items not addressed specifically for privacy but included in the final security regulation are:

- Information Access Management: Isolating Clearing Functions- not applicable.

- Evaluation – while Certification under the proposed rule was not part of the initiative, the requirements for Evaluation will be met through our Security Management Process for Risk Analysis and Risk Management, ongoing internal security audits performed under the direction of our Director of IT Security Audits, audits performed by the organization's Internal Audit Department, which include those performed by external auditing firms, and ongoing penetration tests for systems identified as high risk.

- Contingency Planning – all components were already in place. Additional improvements are planned for more extensive coverage to be able to respond more quickly to disasters.

- Facility Access Controls – all components were already in place. Improvements are planned for contingency operations.

- Device and Media Controls: Re-use and Data Backup and Storage – the re-use is the only "required" standard not yet implemented. Most of the devices and media are handled by a third party thus covered under the disposal standard. Re-use of desktops still needs to be addressed, but since PHI primarily resides on the network drives, the risk is considered is considerably lower. The disposal standard will be used as a model for a device and media re-use standard. In addition it will include a certification process for accountability and data backup and storage.

- Access Control: Encryption/decryption - already in place for User IDs and passwords. The use of encryption for other data at rest is currently under a risk analysis evaluation.

- Integrity: Error-correcting memory and magnetic disk storage are considered built-in data authentication mechanisms in place today. A risk analysis is planned to address any other data that may need other methods of data authentication, such as digital signature or checksum.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

While procedures have been put in place to tighten security, additional manual labor is required to implement them. There is now justification to look for automated solutions to help with these processes. Some of the technology solutions we are actively planning are an authentication server, vulnerability assessment tools, and identity management solutions. The security culture within our organization has changed significantly with the implementation of the HIPAA requirements. People now know it is everyone's responsibility, and the management and financial support for it is there.

Resources:

Federal Register Part II Department of Health and Human Services Office of the Secretary 45 CFR Parts 160 and 164. "Standards for Privacy of Individually Identifiable Health Information; Final Rule", August 28 2000, Part 8, page 82827 URL http://www.hhs.gov/ocr/part8.pdf

RSA Security. "No Privacy Without Security: The HIPAA Privacy Regulation's Requirement for Security" Page 3. URL: http://www.rsasecurity.com/solutions/health/downloads/NPWOS_WP_0603.pdf

Federal Register Part III Department of Health and Human Services Office of the Secretary 45 CFR Part 142, "Security and Electronic Signature Standards; Proposed Rule", August 12, 1998. Pages 43269:43271 URL: http://www.aspe.hhs.gov/admnsimp/nprm/secnprm.pdf

ISO17799 Information Security Group, "The ISO 17799 Directory". URL: http://www.iso-17799.com

OCR HIPAA Privacy, "Minimum Necessary [*45 CFR 164.502(b), 164.514(d)*]", *December 3, 2002, Revised April 4, 2003. Page 1.* URL: http://www.hhs.gov/ocr/hipaa/guidelines/minimumnecessary.pdf

Hardwick, Steve, "Secure Removal of Protected Health Information: Cleaning Hard Drives to the HIPAA Standard Prior to Disposal or Donation", Phoenix Health Systems, HIPAAdvisory.com URL: http://www.hipaadvisory.com/tech/data_removal.htm

Phoenix Health Systems, "Disk Sanitization" , HIPAAdvisory.com URL: http://www.hipaadvisory.com/tech/disksan.htm

Federal Register Part II Department of Health and Human Services, Office of the Secretary 45 CFR Parts 160, 162, and 164, "Health Insurance Reform: Security Standards; Final Rule". February 20, 2003. Page 8380. URL: http://aspe.hhs.gov/admnsimp/FINAL/FR03-8334.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**