Global Information Assurance Certification Paper

Will Implementing the HIPAA Security Rule Protect ePHI for Health Care Providers?

Dan Aiken
February 3, 2004

GSEC Practical Assignment
Version 1.4b, Option 1

Table of Contents

Abstract

The HIPAA final Security Rule was published on February 20, 2003. This rule sets federal standards for safeguarding electronic protected health information, or ePHI (see Appendix C – Definitions). Most health plans, all health care clearinghouses, and most health care providers must comply with these standards by April 21, 2005. Small health plans have until April 21, 2006 to comply; health care providers who do not transmit health information in electronic form in connection with transactions outlined in the HIPAA legislation are not covered entities and are not subject to the legislation at all.

This paper will examine the HIPAA Security Rule against the material covered in the SANS Security Essentials course to see if being compliant with the HIPAA Security Rule is sufficient to assure adequate security for ePHI. This paper will evaluate a few elements that may be missing from the HIPAA final Security Rule and recommend appropriate actions that health care providers should consider to assure appropriate security for ePHI.

Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191, was signed into law by President Bill Clinton on August 21, 1996. HIPAA was written to:

- improve the portability and continuity of health insurance coverage;
- combat waste, fraud, and abuse in health insurance and health care delivery;
- reduce health care costs and administrative burdens by standardizing many administrative and financial transactions, code sets, and national identifiers; and
- protect confidential health care information by setting standards for the privacy and security of protected health information.

In Title II, Subtitle F of the legislation, congress added Section C to Title XI of the Social Security Act (hereafter referred to as the Act), entitled Administrative Simplification.

> The purpose of subtitle F is to improve the Medicare program under title XVIII of the Act, the Medicaid program under title XIX of the Act, and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements to enable the electronic exchange of certain health information. (CMS, p.8334)

HIPAA legislation Section 1173(d), Security Standards for Health Information, requires the development of security standards for health information:

> (1) SECURITY STANDARDS. — The Secretary shall adopt security standards that —
> (A) take into account —
> (i) the technical capabilities of record systems used to maintain health information;
> (ii) the costs of security measures;

(iii) the need for training persons who have access to health information;
(iv) the value of audit trails in computerized record systems; and
(v) the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary); and

(B) ensure that a health care clearinghouse, if it is part of a larger organization, has policies and security procedures which isolate the activities of the health care clearinghouse with respect to processing information in a manner that prevents unauthorized access to such information by such larger organization.

(2) SAFEGUARDS. — Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards —

(A) to ensure the integrity and confidentiality of the information;
(B) to protect against any reasonably anticipated —
(i) threats or hazards to the security or integrity of the information; and
(ii) unauthorized uses or disclosures of the information; and
(C) otherwise to ensure compliance with this part by the officers and employees of such person. (HIPAA)

The Privacy Rule places an implied security requirement on covered entities.

> (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. (OCR, p.39)

The proposed HIPAA Security Rule was published on August 12, 1998. The final HIPAA Security Rule (hereinafter called the Rule) was published on February 20, 2003. All covered health care providers must be compliant with this rule by April 21, 2005. (CMS, p.8334)

HIPAA Security Rule

The Rule is composed of the following sections:

- § 164.302 Applicability
- § 164.304 Definitions
- § 164.306 Security Standards: General Rules
- § 164.308 Administrative Safeguards
- § 164.310 Physical Safeguards
- § 164.312 Technical Safeguards
- § 164.314 Organizational Requirements
- § 164.316 Policies and Procedures and Documentation Requirements

- § 164.318 Compliance Dates for the Initial Implementation of the Security Standards

Sections 164.306–316 will be examined to see how they provide for the security of ePHI.

All standards in the Security Rule must be implemented as specified by covered entities. In addition, many of the standards include implementation specifications, which are either required or addressable. When an implementation specification is required, the covered entity must implement it as specified. When an implementation specification is addressable, the covered entity must assess whether the implementation specification is a reasonable and appropriate safeguard in its environment. If it is, it must be implemented as specified. Otherwise, the covered entity must document why the implementation specification is not reasonable and appropriate in its environment, how the standard is being met, and implement an equivalent alternative measure if reasonable and appropriate. (OCR, p.13; CMS, p.8336) The output of the risk analysis will be critical to the evaluation of all addressable implementation specifications.

The Rule allows great flexibility in how standards and implementation specifications are implemented. The covered entity is permitted to use any security measures that allow it to reasonably and appropriately implement the standards and implementation specifications. In deciding which security measures are reasonable and appropriate, the covered entity may consider its size, complexity, and capability (an individual provider would not be expected to implement the same security measures as a large academic medical center), the covered entity's technical infrastructure, the costs of security measures, and the probability and criticality of the risks it faces. (OCR, p.13)

Appendix A shows a table of the standards and associated implementation specifications for the Administrative Safeguards, Physical Safeguards, and Technical Safeguards sections of the Rule. All standards are required. Each implementation specification is either required (R) or addressable (A).

HIPAA Security Standards and Implementation Specifications

Most attention has been focused on the following sections of the Rule: § 164.308 *Administrative Safeguards*, § 164.310 *Physical Safeguards*, and § 164.312 *Technical Safeguards*, and rightly so, since these sections directly affect the security of ePHI. However, we cannot overlook § 164.306 *Security Standards: General Rules*; § 164.314 *Organizational Requirements*; and § 164.316 *Policies and Procedures and Documentation Requirements*. Each of these sections also specifies standards and implementation specifications for security of ePHI. In addition, § 164.105 *Organizational Requirements* includes requirements that apply specifically to hybrid entities and affiliated covered entities (see Appendix C – Definitions).

Section 164.306 provides the foundational requirement for security of ePHI:

(a) *General requirements.* Covered entities must do the following:
(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part [the Privacy Rule].
(4) Ensure compliance with this subpart by its workforce. (OCR, p.13)

It also establishes a requirement for ongoing review and modification of security measures to assure continuing protection of ePHI:

(e) *Maintenance.* Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described in § 164.316. (OCR, p.13)

Section 164.314 provides a standard and implementation specifications for Business Associate agreements. This provides some assurance that ePHI will be appropriately safeguarded when provided to individuals or organizations who are not HIPAA covered entities. This is important since covered entities regularly provide ePHI to outside persons or organizations, including attorneys, transcription services, billing services, consulting firms, etc. (OCR, pp.15–16)

Section 164.316 provides standards and implementation specifications for documentation and policies and procedures. Security policies and procedures set the overall tone and authority for information security, and provide specific direction on how security measures will be implemented within the organization. (OCR, p.16)

Security Essentials vs. the Security Rule

The Security Rule has a considerable dependence on the risk assessment. In the Preamble, it mentions that elements not included in the Rule (e.g., configuration management) may still be required depending on the results of the risk assessment. (CMS, p.8352) Also, the implementation of the addressable elements of the Rule depends on the results of the risk assessment. Therefore, in the following analysis a missing security element may still be implicitly required for HIPAA compliance.

A cross reference of the Security Rule to security requirements contained in the Security Essentials course is contained in Appendix B. This cross reference is the basis for the following analysis. Security Essentials material for days 5 and 6 (Windows Security and Unix Security) are not included in this analysis since they are operating system-specific implementations of the material already covered in the training.

1. **Network Design** – The Rule makes no explicit mention of network security principles such as resource separation, firewall placement and protection, and limiting visibility of traffic between systems.
2. **IP Concepts I** – This chapter provides some basic concepts that are necessary to understand security. No crosswalk with the Rule is necessary.
3. **IP Concepts II**

3.1. **Network Scanning** – There is no explicit mention of scanning the entity's network to limit ports and services to those necessary to the organization's mission. The requirement to do network scanning should be identified by the Risk Analysis process.

4. **IP Behavior**

4.1. **Network Scanning** – There is no explicit mention of network scanning in the Rule. This capability is important, however, to comply with the identification of security incidents requirement of the Security Incident Procedures standard (see Incident Handling Foundations below).

4.2. **Know Your Network** – While this fundamental security practice is not part of the Rule, it is important to be able to comply with the Security Incident Procedures standard.

5. **Routing Fundamentals**

5.1. **Packet Filtering** – By design, no mention is made of the security practice to filter inbound and outbound packets. This requirement would result from the risk analysis process.

6. **Physical Security**

6.1. **Physical Safety** – The Rule makes no mention of the need to assure the safety of personnel.

6.2. **Authorized Access** – The rule covers physical access security in a comprehensive way. It has several elements for securing the physical access to ePHI systems and facilities: contingency operations, facility security plan, access control and validation procedures, and maintenance records. The Rule also requires physical safeguards to control access to workstations that access ePHI. (CMS, p.8378) Careful consideration should be given to portable devices to assure the protection of ePHI that may be stored on the device.

7. **Defense in Depth**

7.1. **Confidentiality, Integrity, and Availability** – All three categories of security are covered generally in § 164.306(a)(1)–(4). Integrity is also covered under Technical Safeguards. The Rule clearly requires the assurance of confidentiality, integrity, and availability of ePHI data and systems.

7.2. **Identity, Authentication, and Authorization** – The rule covers identity, authentication, and authorization under Administrative and Technical Safeguards. It requires that access to ePHI be consistent with the standards of the Privacy Rule. It specifically requires the isolation of access to ePHI in clearinghouse functions within a larger organization; the authorization, establishment, and modification of access rights to ePHI, and the technical implementations to support those rights; unique user identification, emergency access procedures, automatic logoff, and encryption and decryption of data at rest; entity or person authentication;

and the protection against unauthorized access to ePHI being transmitted, including the assurance of the integrity of data being transmitted and encryption of that data as appropriate based on the organization's risk assessment.

7.3. **Threats, Vulnerabilities, and Risks** – See Risk Management and Auditing below.

7.4. **Configuration Management** – Configuration management is not specifically mentioned in the final version of the Rule. However, in the Preface to the Rule, HHS explained why they decided to drop this requirement.

> Upon review, [security configuration management] appears unnecessary because it is redundant of other requirements we are adopting in this rule. A covered entity will have addressed the activities described by the features under this proposed requirement by virtue of having implemented the risk analysis, risk management measures, sanction policies, and information systems criticality review called for under the security management process. (CMS, p.8352)

8. **Basic Security Policy** – The Rule requires reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule.

8.1. **Documentation** – The Rule requires that policies, procedures, actions, activities, and assessments required by the Security Rule be maintained in written (which may be electronic) form and be retained for at least six years.

8.2. **Anti-Virus** – As a part of the security awareness and training requirement, the Rule requires procedures for guarding against, detecting, and reporting malicious software. The rule does not include any specific implementation requirements to protect against malicious software, but those details would be developed as a result of the required risk analysis and risk management processes.

8.3. **Password Assessment** – The rule does not require that the covered entity perform any password assessment activity, although it could be seen as a part of the general requirement of § 164.306(a)(4) to ensure compliance by the workforce with the elements of the Security Rule.

8.4. **Data Backup** – As a part of the requirement for a contingency plan, the Rule requires the covered entity to establish and implement procedures to create and maintain backup copies of ePHI. The backup of other data could be covered under the requirement for contingency planning.

8.5. **Proprietary Information** – The Plan is only concerned with the protection of ePHI. It makes no requirement for the protection of other types of proprietary information (financial records, medical research data, employee information, etc.).

8.6. **Business Continuity Plan** – The Rule requires the covered entity to establish, and implement as necessary, procedures to enable the continuation of critical business processes to maintain the protection of ePHI during emergency operations. It does not mention the continuation of other business processes which may be necessary for the continued provision of health care and other business operations.

8.7. **Disaster Recovery Plan** – The Rule requires the establishment and implementation as needed of procedures to restore lost data. Other implementation specifications of the contingency planning standard include having a disaster recovery plan, emergency mode operation plan, testing and revision procedures, and an applications and data criticality analysis.

8.8. **Risk Analysis** – The Rule requires that a risk analysis be performed to determine the appropriate implementation of all addressable implementation procedures and many other requirements of the Security Rule. A maintenance requirement that was added to the Rule (§ 164.306(e)) is designed to assure that, among other security measures, the risk assessment will be performed as often as necessary to maintain effective security. (OCR, 8346–7)

8.9. **Business Impact Analysis** – The Rule requires that the covered entity assess the relative criticality of specific applications and data in support of other contingency plans. Since the contingency plan requirement itself only applies to the protection of ePHI, this requirement could also be seen as applying only to ePHI applications and data. A health care provider, of course, has many other applications and associated data that are critical to the provision of health care. It could be appropriate to include these applications and data in the contingency planning activities required by the Rule.

8.10. **Sample Policies**

8.10.1. **Anti-Virus and Work Incidents** – See Anti-Virus above and Incident Handling Foundations below.

8.10.2. **Password Assessment** – See Passwords below.

8.10.3. **Backups** – The Rule requires the development of a data backup plan for ePHI. The details of the data backup plan, including the frequency and retention of backups and the inclusion of non-ePHI data, will come from the risk analysis and risk management activities.

8.10.4. **Incident Handling** – See Incident Handling Foundations below.

8.10.5. **Proprietary Information** – The Rule only covers ePHI. Other types of proprietary information (e.g., financial and research information) are not addressed in the Rule.

9. **Access Control and Password Management** – See Identity, Authentication, and Authorization above.

9.1. **Principle of Least Privilege** – The Security Rule is required to support the requirements of the Privacy Rule (cf. § 164.306(a)(3)), which requires that only the minimum necessary information be available to anyone with access to PHI. The Rule does not, however, cover applications of the principle of least privilege to other data.

9.2. **Passwords** – Password management is part of the Security Awareness and Training standard. It requires procedures for creating, changing, and safeguarding passwords. The details of the password assessment policy (e.g., guidance for strong password selection) are not contained in the Rule. However, this content should come from the required risk analysis and risk management processes.

10. **Incident Handling Foundations** – The Rule requires the implementation of policies and procedures to address and respond to suspected or known security incidents, to reasonably mitigate their effects, and to document the security incidents and their outcomes. The final rule does not require the reporting of security incidents to any outside person or organization.

11. **Information Warfare** – The Rule does not directly address the various persons or groups that may have motivation to attack a covered entity, the methods or tools that may be used in such an attack, or the extent of the possible results. However, many of the protections addressed by the Rule would be effective in preventing many information warfare attacks. For example, the training on malicious code and password management would inform the workforce about these avenues of attack, but the Rule does not directly address social engineering attacks, the vulnerabilities of predictable responses, or false perceptions about the protections offered by implemented security controls (e.g., firewalls and anti-virus software).

12. **Web Communications and Security**

12.1. **Active Content** – The Rule addresses malicious software, but not any particular technology that may be employed. Particular care should be taken, therefore, to address these technologies in the risk analysis effort.

12.2. **Authentication** – The Rule covers person or entity authentication in the Technical Safeguards section. It does not address the special concerns associated with web access. Once again, particular care should be taken to address these concerns in the risk analysis effort.

12.3. **Input Validation** – The Security Rule covers integrity of information from the standpoint of preventing unauthorized modification or deletion, but it does not address integrity from the standpoint of assuring the accuracy of data entry. The risk analysis effort should be sure to address this concern.

12.4. **Web Application Defenses** – The Rule does not address security issues relevant to software development or acquisition, including web applications. This is a major omission of the rule, in my view, and should be carefully considered during the risk analysis process.

13. **Attack Strategies and Mitigation**

13.1. **Prevention** – Much of the Rule is designed to prevent security incidents. This will be driven by the security management process required by the Administrative Safeguards section of the Rule.

13.2. **Detection** – See Host-Based Intrusion Detection and Network-Based Intrusion Detection below.

13.3. **Response** – See Incident Handling Foundations above.

14. **Firewalls and Honeypots** – The Rule by design does not address specific security technologies. It therefore does not address the use, location, or configuration of firewalls or honeypots. These details will have to be addressed by the risk analysis effort.

15. **Vulnerability Scanning** – In the section on risk analysis, the Rule requires a "thorough assessment of the potential risks and vulnerabilities" to the CIA of ePHI. It does not, however specifically mention vulnerability scanning. In the Preface, the Rule mentions the NIST SP 800-30 *Risk Management Guide for Information Technology Systems*, which does make mention of vulnerability scanning as one of several proactive methods which could be used to identify system vulnerabilities. (NIST(2), p.16)

16. **Host-Based Intrusion Detection** – The Rule does not mention specific controls to be used for security purposes, but instead relies on the security management process (§ 164.308(a)(1)) to identify risks and mitigating controls.

17. **Network-Based Intrusion Detection** – Same as above.

18. **Risk Management and Auditing** – The rule requires a security management process that begins with a risk analysis/risk management process. In the Preamble to the Rule, the reader is directed to the NIST SP 800-30, "Risk Management Guide for Information Technology Systems," for more information on performing a risk analysis. (CMS, p8346)

    The auditing requirement is found in several places in the Rule, not always labeled as "auditing." Kurt Patti, in his paper, *HIPAA Security Compliance Project – Identification of Logging and Auditing Requirements*, writes,

    > Included among the Administrative Safeguards section of the rule, is a requirement to conduct an "Information system activity review". This is the terminology selected to replace the terms "internal audit" as required in the proposed regulations. (Patti, p.2)
    >
    > The Administrative Safeguards section also contains a Security Awareness and Training Standard that includes an addressable implementation specification termed "log-in monitoring." "Log-in monitoring," points to creating procedures for monitoring log-in attempts to applications and systems containing PHI, and for reporting discrepancies. (Patti, p.2)
    >
    > A third standard within the Administrative Safeguards section of The Final Rule, related to logging and auditing of electronic PHI is the Evaluation Standard. This standard requires a covered entity to periodically evaluate itself both technically and non-technically, with regard to how it measures up

> to the standards implemented under the Final HIPAA Security Rule. (Patti, p.2–3)
>
> The Technical Safeguards section calls out an "Audit Controls" standard. The Audit Controls standard requires the capability to record and examine system activity in information systems containing, or using electronic protected health information. (Patti, p.3)

19. **Encryption 101** – This chapter provides some basic concepts that are necessary to understand encryption. No crosswalk with the Rule is necessary.
20. **Encryption 102** – This chapter provides additional concepts regarding encryption. No crosswalk with the Rule is necessary.
21. **Applying Cryptography** – The Rule makes encryption of data at rest and across the network addressable implementation specifications. As such, it requires the covered entity to determine appropriate uses of encryption in its environment.
22. **Steganography** – By design, the Rule is not technology specific, and therefore makes no mention of the techniques and tools of steganography.
23. **Viruses and Malicious Code** – The Rule makes training on protection from malicious software an addressable implementation specification. It does not directly address the technical controls that should be used to provide protection from malicious code. The need for specific controls should be identified during the risk analysis and risk management processes.
24. **Operations Security**
    - 24.1. **Legal Requirements** – The legal requirements of the Rule include organizational requirements for hybrid entities and affiliated covered entities, supporting the requirements of the Privacy Rule, isolating any clearinghouse functions from unauthorized access by the rest of the organization, periodically evaluating the extent to which policies and procedures continue to meet the requirements of the Rule, establishing business associate contracts, and meeting specific requirements for group health plans. While it may seem that this last requirement does not apply to health care providers, certain types of employee health benefit plans offered by employers meet the definition of a group health plan under HIPAA. Because the Rule focuses on ePHI, it does not include legal requirements regarding copyrights, retention of records, due care, or due diligence.
    - 24.2. **Privacy and Protection** – The Rule requires implementation of measures to support the requirements of the Privacy Rule, which is only concerned with the privacy and protection of PHI.
    - 24.3. **Illegal Activities** – The HIPAA legislation includes section 1177, *Wrongful Disclosure of Individually Identifiable Health Information*. The Rule includes no specific requirements regarding other illegal activities.

24.4. **Job Requirements** – This is not required by the rule. It could be a requirement that comes out of the required risk analysis and risk management processes.

24.5. **Background Checking** – Same as above.

24.6. **Separation of Duties** – Same as above.

24.7. **Job Rotation** – Same as above.

24.8. **Vacation and Leave** – Same as above.

24.9. **Terminations** – The Rule includes the requirement to terminate access to ePHI for terminated employees or when required by a person's changing access requirements. It does not include other security requirements regarding terminations (recovery of keys, badges, property, etc.)

24.10. **Employment Agreements** – This is not required by the rule. It could be a requirement that comes out of the required risk analysis and risk management processes.

24.11. **Individual Accountability** – The Rule requires unique user identification, permitting the logging and auditing of individual access and activity. It also requires a sanctions policy that applies "appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity," thus requiring individual accountability (§ 164.308(a)(1)(ii)(C)).

24.12. **Need to Know** – The Rule includes the following two standards that work together to provide for need to know for ePHI. The Rule does not cover need to know for other types of data. This should be considered during the risk analysis effort.

24.12.1. **Assigned Security Responsibility** – This standard requires policies and procedures that assure "appropriate access" (as provided under the Information Access Management standard) to ePHI by members of its workforce.

24.12.2. **Information Access Management** – This standard requires policies and procedures for authorizing access to ePHI that are consistent with the requirements of the Privacy Rule.

24.13. **Sensitive Information** – The only sensitive information protected the Rule is ePHI. Other sensitive information should be considered during the risk analysis process.

24.14. **Operations Controls** – The Rule requires physical safeguards for hardware, software, data, and media.

Monitoring and Auditing – See the auditing comments under Risk Management and Auditing.

24.15. **Roles and Responsibilities** – The Rule includes the requirement to identify the security official who is responsible for the development and

implementation of the policies and procedures required by the Rule. It does not address the roles and responsibilities of users, system owners, etc., nor does it address other appropriate responsibilities of the security official.

24.16. **Training and Awareness** – The Rule requires a security training and awareness program, including specific requirements for security reminders and training in protection from malicious software, log-in monitoring, and password management. A complete security training and awareness program will include many additional topics.

HIPAA in the Final Analysis

Now that we have compared the Rule to the Security Essentials course content, let's consider what may be missing, and how critical that could be to the security of ePHI.

The purpose of information security is to assure the confidentiality, integrity, and availability of information to support the mission of the organization.

The HIPAA Security Rule, on the other hand, is written to assure the confidentiality, integrity, and availability of the organization's ePHI; to protect against any reasonably anticipated threats or hazards to ePHI; to provide the tools necessary to implement the requirements of the Privacy Rule; and to ensure compliance with the Security Rule by its workforce (§ 164.306(a)(1)). The Security Rule is only concerned with the security of ePHI.

This means that implementing security only as required by the Security Rule could leave other information assets vulnerable and the organization at risk. For example, if the risk assessment is only concerned with systems that store and process ePHI, other systems (e.g., accounts payable, payroll, asset tracking, purchasing, etc.) could be left with inadequate security safeguards. This is a weakness in the Rule from the standpoint of overall information security.

With this in mind, it is nevertheless true that the focus of this analysis is on protecting ePHI, so we will proceed with our evaluation of the rule primarily from the standpoint of its ability to protect ePHI.

The general requirements of § 164.306(a)—(1) to ensure the confidentiality, integrity, and availability of ePHI; (2) to protect against *any reasonably anticipated* threats or hazards to the security or integrity of ePHI; (3) to protect against any reasonably anticipated uses or disclosures which are not permitted under the Privacy Rule; and (4) to ensure compliance by the covered entity's workforce—are very broad and probably impossible to meet. According to the National Institute of Standards and Technology (NIST),

> It is estimated that ninety-nine percent of all reported intrusions result through exploitation of known vulnerabilities or configuration errors, for which safeguards and countermeasures were available. (NIST, p. 1)

This means that ninety-nine percent of all reported intrusions could have been *reasonably anticipated*, and would have been a violation of § 164.306(a). Therefore, the risk analysis and risk management requirements of the Rule are vitally important. Anticipating and mitigating risks is the name of the game.

The following Security Essentials topics are not directly addressed by the Rule, but could be addressed during the risk analysis and risk management processes: network design, packet filtering, personnel safety, configuration management, separation of duties, social engineering attacks, web communications active content and input validation, application development, firewalls and honeypots, host- and network-based intrusion detection, steganography, protective controls for malicious software, illegal activities other than wrongful disclosure of ePHI, defining job requirements, background checking, separation of duties, job rotation, vacation and leave, employment agreements, and roles and responsibilities other than the Security Officer. In addition each addressable implementation specification must be considered in light of its contribution to security for that covered entity.

It is apparent, therefore, that risk analysis and risk management are vital to the successful implementation of the requirements of the Rule. In her analysis of the impacts of privacy and security under HIPAA, Barbara Filkins agreed when she wrote,

> The *risk analysis and risk management processes* required by §164.308 are critical to defining the measures against which the [covered entity's] implementation of HIPAA security would be assessed. Additionally, other sections of the rule reemphasize the criticality of a strong, well-documented risk analysis. (Filkins, p.15)

In my judgment, the following security topics should be given careful consideration during the risk analysis process.

Personnel Safety Issues

Personnel safety should be an important consideration of physical security. Therefore, threats to personnel safety should be given a prominent place in the risk analysis process.

Application Development

It is important to make security an important consideration from the earliest phases of the software development process. Adding security controls and features at the later phases of the process has proven to be a time consuming, error prone, and expensive process, and would likely not be as effective after all that. Application development security issues should be an important part of the risk analysis process.

Configuration Management

If you can't control the configuration of your network and its controls, you can be sure that your desired security level will be maintained. Configuration management must be an important part of the risk analysis process.

Backups

The rule explicitly requires backing up ePHI, but the backing up of other data, programs, and configurations will be a vital part of the disaster recovery plan, also. The details should be carefully reviewed during the risk analysis process.

Intrusion Detection Systems

An intrusion detection system (IDS) is an important part of network security. E. Eugene Schultz and Eugene Spafford, in their chapter on intrusion detection in the 4th edition of the Information Security Management Handbook, say,

> An inherent danger in the incident response arena is the implicit assumption that if no incidents surface, all is well. Superficially this assumption seems logical. Studies by the U.S. Defense Information Systems Agency (DISA) in 1993 and again in 1997, however, provide statistics that prove it is badly flawed. Van Wyk [VANW94] found that of nearly 8800 intrusions into Department of Defense systems by a DISA tiger team, only about one in six was detected. Of the detected intrusions, approximately only 4 percent were reported to someone in the chain of command. This meant that of all successful attacks, less that 1 percent were both noticed and reported. (Schultz, p.682)

A vital part of the incident response capability is the ability to detect attacks. Not seeing attacks does not mean that there are no attacks. We need to include an appropriate tool to detect them more successfully. This should be an important consideration during the risk analysis and risk management processes.

Applying Cryptography

The use of encryption for data at rest (§ 164.312(a)(2)(iv)) and data in motion (§ 164.312(e)(2)(ii)) are both addressable implementation specifications, meaning that they will need to be implemented in light of the results of the risk analysis process. Of particular concern is data that is transmitted across the internet, e.g., in e-mails sent to addresses outside of the entity's network. This should be carefully considered during the risk analysis process.

Malicious Code

The selection and implementation of controls to protect against malicious code must be an important part of the risk analysis process. Virus detection at both the server and workstation and the use of more than one vendor's software are examples of defense in depth and should also be considered during risk analysis.

Operation Security

Job requirements, background checking, separation of duties, job rotation, vacation and leave, and employment agreements should be considered during risk analysis.

Conclusions

I have reached four primary conclusions.

1. It is not possible to comply with the Rule without also effectively protecting ePHI. Even if the specific standards and implementation specifications don't require all that is necessary for the security of ePHI, § 164.306(a) still requires the covered entity to do everything that the risk analysis and risk management processes determine is necessary to protect ePHI. The risk analysis and risk management

processes will be vital in assuring that all necessary security controls are in place to reduce risk to an acceptable level.

2. There are some significant intentional and unintentional omissions from the Rule, most importantly personnel security, configuration management, and application development. These should be given careful consideration during risk analysis.
3. It is important to realize that the Rule only considers ePHI. Other vital security concerns may be overlooked. Therefore, while it may not be possible to be compliant with the Rule without providing effective security for ePHI, the Rule does not assure that all necessary security concerns will be met.
4. There are many other areas where the need for controls, as well as their selection and implementation, will depend on the risk analysis and risk management activities. See the detailed sections in HIPAA in the Final Analysis above for more information.

Recommendations

1. Perform a careful and complete risk analysis. There are many places in the Rule that depend on the conclusions of the risk analysis and risk management processes to guide you in protecting ePHI.
2. Keep in mind that the Security Rule is only concerned with the protection of ePHI. There may be other important organizational interests that need protection, also.
3. Do not limit your initial focus to the protection of ePHI. You may decide to limit your initial implementation efforts to HIPAA concerns, but you should know what other areas still need attention. Some of them may be able to be addressed at the time of your initial HIPAA compliance efforts.

Appendixes

Appendix A — Security Standards: Matrix

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure (A) Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement.	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

(CMS, p.8380)

Appendix B — Security Essentials

Because the HIPAA Security Rule is designed to be technically neutral, this paper will not evaluate the Security Rule against technical implementation details in the course such as networking technology in Week 1 and Windows and Unix security in Weeks 5 and 6. We will, however, evaluate the rule against the general topics covered in those sessions.

Course Topic	Week	Security Rule Reference
Network Design	1a	
Resource separation		
Firewall placement and protection		
Limiting visibility of traffic between systems		
IP Concepts I	1a	
IP Concepts II	1a	
Network scanning		
IP Behavior	1b	
Routing Fundamentals	1b	
Packet filtering		
Physical Security	1b	
Safety		
Authorized access		§ 164.310(a)(1) § 164.310(a)(2)(i)–(iv)
Defense in Depth	2a	
Confidentiality, integrity, and availability		§ 164.306(a)(1)–(4) § 164.312(c)(1) § 164.312(c)(2)
Identity, authentication, and authorization		§ 164.308(a)(4)(i) § 164.308(a)(4)(ii)(A)–(C) § 164.312(a)(1) § 164.312(a)(2)(i)–(iii) § 164.312(d) § 164.312(e)(2)(i)
Threats, vulnerabilities, and risks		§ 164.308(a)(1)(ii)(A)–(B)
Configuration management		Preface III.9.a
Basic Security Policy	2a	§ 164.316(a)
Documentation		§ 164.316(b)(1)(i)–(ii)
Anti-Virus		§ 164.308(a)(5)(ii)(B)
Password Assessment		
Data Backup		§ 164.308(a)(7)(ii)(A)
Proprietary Information		
Business Continuity Plan		§ 164.308(a)(7)(C)
Disaster Recovery Plan		§ 164.308(a)(7)(B)
Risk Analysis		
Business Impact Analysis		§ 164.308(a)(7)(E)
Sample Policies		
Acceptable Encryption		§ 164.312(a)(2)(iv) § 164.312(e)(2)(ii)
Acceptable Use		§ 164.310(b)
Anti-Virus Guidelines		§ 164.308(a)(5)(ii)(B)

Course Topic	Week	Security Rule Reference
Acquisition Assessment		
Audit		§ 164.308(a)(1)(ii)(D) § 164.312(b)
Automatically Forwarded E-Mail		
Dial-in Access		
Extranet		
Information Sensitivity		
Password		§ 164.308(a)(5)(ii)(D)
Remote Access		
Risk Assessment		§ 164.308(a)(1)(ii)(A)
Virtual Private Network		
Wireless Communications		
Access Control and Password Management	2a	§ 164.308(a)(4)(i) § 164.308(a)(4)(ii)(B)–(C)
Separation of duties		
Principle of Least Privilege		§ 164.308(a)(4)(i)
Passwords		§ 164.308(a)(5)(ii)(D)
Incident Handling Foundations	2b	§ 164.308(a)(6)(i)–(ii) § 164.308(a)(1)(ii)(D)
Information Warfare	2b	
Web Communications and Security	2b	
Active content		
Authentication		§ 164.312(d)
Input validation		
Web application defenses		
Internet Security Technologies	3a	
Firewalls and Honeypots	3a	§ 164.308(a)(5)(ii)(B)
Vulnerability Scanning	3a	§ 164.308(a)(5)(ii)(B)
Host-based Intrusion Detection	3b	§ 164.308(a)(5)(ii)(B)
Network-based Intrusion Detection	3b	§ 164.308(a)(5)(ii)(B)
Risk Management and Auditing	3b	§ 164.308(a)(1)(ii)(A)–(B) § 164.308(a)(5)(ii)(C) § 164.312(b)
Secure Communications	4a	
Encryption 102	4a	
Applying Cryptography	4a	§ 164.312(a)(2)(iv) § 164.312(e)(2)(ii)
Steganography	4b	
Viruses and Malicious Code	4b	§ 164.308(a)(5)(ii)(B)
Operations Security	4b	
Legal Requirements		§ 164.105 § 164,306(a)(3) § 164.308(a)(4)(ii)(A) § 164.308(a)(8) § 164.308(b)(1)–(4) § 164.314(a) § 164.314(b)
Privacy and Protection		§ 164.306(a)(3)
Illegal Activities		Sec. 1177 of the Legislation
Job requirements		

Course Topic	Week	Security Rule Reference
Background checking		
Separation of duties		
Job rotation		
Vacation and leave		
Terminations		§ 164.308(a)(3)(ii)(C)
Employment agreements		
Individual accountability		§ 164.308(a)(1)(ii)(C)
Need to know		§ 164.308(a)(4)(i)
Sensitive information		§ 164.308(a)(4)(i)
Operations Controls		§ 164.310((a)(2)(ii) § 164.310(d)(1)–(2)(iv)
Monitoring and Auditing		§ 164.308(a)(1)(ii)(D) § 164.308(a)(5)(ii)(C) § 164.312(b)
Roles and Responsibilities		§ 164.308(a)(2)
Training and awareness		§ 164.308(a)(5)(i)–(ii)(D)

Appendix C — Definitions

Affiliated Covered Entities are legally separate covered entities that choose to designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of the Security Rule and the Privacy Rule, if all of the covered entities designated are under common ownership or control. (OCR, p.12)

Covered Entity means:

(1) A health plan.
(2) A health care clearinghouse.
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. (OCR, pp.1–2)

Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information. (OCR, p.2)

Electronic Protected Health Information means *protected health information* that is transmitted by or maintained in electronic media. (OCR, p.2)

Hybrid Entity means a single legal entity:

(1) That is a covered entity;
(2) Whose business activities include both covered and non-covered functions; and
(3) That designates health care components in accordance with the requirements of the Rule. (OCR, p.11)

Individually Identifiable Health Information is health information, including demographic information that is collected from an individual, and:

(1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
    (i) that identifies the individual; or
    (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. (OCR, p.3)

Protected Health Information means individually identifiable health information:

(1) held by a covered entity except as provided in paragraph (2) of this definition, that is:
    (i) transmitted by electronic media;
    (ii) maintained in electronic media; or
    (iii) transmitted or maintained in any other form or medium.
(2) Protected health information excludes individually identifiable health information in:
    (i) education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
(iii) employment records held by a covered entity in its role as employer. (OCR, p.3)

Use means, with respect to protected health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. (OCR, p.4)

References

CMS (Centers for Medicare and Medicaid Services). "Health Insurance Reform: Security Standards; Final Rule." Federal Register, Vol. 68, No. 34, Part II, Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160, 162, and 164. February 20, 2003. URL: www.aspe.hhs.gov/admnsimp/FINAL/FR03-8334.pdf (October 11, 2003)

Filkins, Barbara. "Getting Started: The Impacts of Privacy and Security Under HIPAA – A Case Study." SANS Reading Room. July 10, 2003. URL: http://www.sans.org/rr/papers/index.php?id=1214 (January 29, 2004)

HIPAA. "Health Insurance Portability and Accountability Act of 1996." Public Law 104-191. August 21, 1996. URL: aspe.hhs.gov/admnsimp/pl104191.htm (October 12, 2003)

NIST (National Institute of Standards and Technology). "Recommended Security Controls for Federal Information Systems." NIST Special Publication 800–53, Technology Administration, Department of Commerce, Initial Public Draft. October 2003. URL: csrc.nist.gov/publications/drafts/draft-SP800-53.pdf (November 23, 2003)

NIST(2) (National Institute of Standards and Technology). "Risk Management Guide for Information Technology Systems." NIST Special Publication 800–30 Rev A, Technology Administration, Department of Commerce. January 2004. URL: http://csrc.nist.gov/publications/drafts/SP800-30-RevA-draft.pdf (January 30, 2004)

OCR (Office of Civil Rights). "Standards for Privacy of Individually Identifiable Health Information; Security Standards for the Protection of Electronic Protected Health Information; General Administrative Requirements Including, Civil Money Penalties: Procedures for Investigations, Imposition of Penalties, and Hearings." Department of Health and Human Services, Regulation Text (Unofficial Version), 45 CFR Parts 160 and 164, as amended: May 31, 2002, August 14, 2002, February 20, 2003, and April 17, 2003. URL: www.hhs.gov/ocr/combinedregtext.pdf (October 12, 2003)

Patti, Kurt. "HIPAA Security Compliance Project – Identification of Logging and Auditing Requirements." SANS Reading Room, August 27, 2003. URL: http://www.sans.org/rr/papers/index.php?id=1227 (January 30, 2004)

Schultz, E. Eugene, and Eugene Spafford. "Intrusion Detection: How to Utilize a Still Immature Technology", *Information Security Management Handbook.* 4th ed. Harold F. Tipton and Micki Drause, eds. New York: Auerbach, 2000. 681–696.