
WEDI - Strategic National Implementation Process (SNIP)

Risk Analysis White Paper



SNIP

**Risk Analysis White Paper
Working Draft Version 1.0 – July 2004**

SNIP Security and Privacy Workgroup

Workgroup for Electronic Data Interchange

12020 Sunrise Valley Drive., Suite 100, Reston, VA 20191

(t) 703-391-2716 / (f) 703-391-2759

© 2004 Workgroup for Electronic Data Interchange, All Rights Reserved

Contents

- Risk Analysis 1**
- Disclaimer 1
- White Paper Background and Overview 1
- Risk Analysis Requirements 2
- How to Approach the Risk Analysis Process 3
- Specific Security Rule Requirements 5
- Standards and Implementation Specifications 5
- “Required” and “Addressable” 6
- Administrative Safeguards 6
- Standard: Security Management Process 7
- Implementation Specification: Risk Analysis (Required) 7
- Implementation Specification: Risk Management (Required)..... 7
- Implementation Specification: Sanction Policy (Required)..... 8
- Implementation Specification: Information System Activity Review (Required)..... 8
- Standard: Assigned Security Responsibility 9
- Standard: Workforce Security 9
- Implementation Specification: Authorization and/or Supervision (Addressable) 9
- Implementation Specification: Workforce Clearance Procedure (Addressable) 10
- Implementation Specification: Termination Procedures (Addressable) 10
- Standard: Information Access Management 11
- Implementation Specification: Isolating Health care Clearinghouse Function (Required)..... 11
- Implementation Specification: Access Authorization (Addressable) 12
- Implementation Specification: Access Establishment and Modification (Addressable) 12
- Standard: Security Awareness and Training 13
- Implementation Specification: Security Reminders (Addressable)..... 13
- Implementation Specification: Protection from Malicious Software (Addressable) 14
- Implementation Specification: Log-in Monitoring (Addressable)..... 14
- Implementation Specification: Password Management (Addressable)..... 15
- Standard: Security Incident Procedures..... 15
- Implementation Specification: Response and Reporting (Required)..... 15

Standard: Contingency Plan	17
Implementation Specification: Data Backup Plan (Required)	17
Implementation Specification: Disaster Recovery Plan (Required)	18
Implementation Specification: Emergency Mode Operation Plan (Required)	18
Implementation Specification: Testing and Revision Procedure (Addressable)..	18
Implementation Specification: Applications and Data Criticality Analysis (Addressable)	19
Standard: Evaluation	19
Standard: Business Associate Contracts and Other Arrangement.....	20
Physical Safeguards	21
Standard: Facility Access Controls	21
Implementation Specification: Contingency Operations (Addressable).....	21
Implementation Specification: Facility Security Plan (Addressable)	22
Implementation Specification: Access Control and Validation Procedures (Addressable)	22
Implementation Specification: Maintenance Records (Addressable).....	23
Standards: Workstation Use and Workstation Security	23
Standard: Device and Media Controls.....	24
Technical Safeguards	26
Standard: Access Control	26
Implementation Specification: Unique User Identification (Required).....	26
Implementation Specification: Emergency Access Procedure (Required)	27
Implementation Specification: Automatic Log-off (Addressable)	27
Implementation Specification: Encryption and Decryption (Addressable)	28
Standard: Audit Controls.....	28
Standard: Integrity	28
Implementation Specification: Mechanism to Authenticate Electronic Protected Health Information (Addressable).....	29
Standard: Person or Entity Authentication	29
Standard: Transmission Security.....	30
NIST/URAC/WEDI Initiative	31
Other Sources of Information.....	32
Acknowledgments	32
Appendix A: Security Standards Matrix	33

Risk Analysis

Disclaimer

This document is Copyright © 2004 by The Workgroup for Electronic Data interchange (WEDI). It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. This document is provided "as is" without any express or implied warranty.

While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by the Workgroup for Electronic Data Interchange. The listing of an organization does not imply any sort of endorsement and the Workgroup for Electronic Data Interchange takes no responsibility for the products, tools, and Internet sites listed.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by the Workgroup for Electronic Data Interchange (WEDI), or any of the individual workgroups or sub-workgroups of the Strategic National Implementation Process (SNIP).

Document is for Education and Awareness Use Only

The HIPAA Security and Privacy requirements are designed to be ubiquitous, technology neutral and scalable from the very largest of health plans, to the very smallest of provider organizations. As the Privacy Rule and Security Rule relate to policies and procedures, many covered entities will find compliance not an application of exact template processes or documentation, but rather a remediation based on a host of complex factors unique to each organization.

White Paper Background and Overview

The Risk Analysis Sub-workgroup was formed following the release of the final Security Rule. This white paper addresses the final Security Rule requirement that all HIPAA “covered entities” perform a security “risk analysis.” The white paper discusses solutions various covered entities can consider adopting to meet the requirement to complete a risk analysis.

In order to begin the Risk Analysis process, one must first review the final Security Rule in general and its guidance regarding HIPAA security implementation. The following excerpts from the final rule and preamble give a clear understanding of the rule requirements and an idea of how to approach compliance.

Section 164.306, Security standards: General rules, states that covered entities must:

- ensure the *confidentiality, integrity, and availability* of all electronic protected health information (ePHI) the covered entity creates, receives, maintains, or transmits;
- *protect against any reasonably anticipated threats or hazards* to the security or integrity of such information;
- *protect against any reasonably anticipated uses or disclosures* of such information that are not permitted or required under subpart E of this part; and
- ensure compliance with this subpart by its workforce.

Remember that the flexibility of the approach is both the greatest advantage and probably the toughest challenge in the rule. Specifically:

- Covered entities may use *any security measures* that allow the covered entity to *reasonably and appropriately* implement the standards and implementation specifications as specified in this subpart.
- In deciding which security measures to use, a covered entity must take into account the following factors:
 - the *size, complexity, and capabilities of the covered entity*;
 - the covered entity's *technical infrastructure*, hardware, and software *security capabilities*;
 - the *costs of security* measures; and
 - the *probability and criticality of potential risks* to electronic protected health information.

The fact that the rule recommends no specific technological solution will cause organizations to differ in their solution choices. These differences will be most significant between different kinds of entities and different size entities. For example, the approach taken by a small practice will necessarily be very different from a multi-hospital system and a large health plan. The rule is written with flexibility to allow covered entities the ability to tailor compliance strategies to their specific circumstances. While this paper attempts to offer suggestions for an entity's consideration, it is recognized that making "one size fits all" recommendations may undermine the general regulatory goal of flexibility. This flexibility results from comments received in response to the proposed Security Rule:

We have received numerous comments expressing the view that the security standards should not be overly prescriptive because the speed with which technology is evolving could make specific requirements obsolete and might in fact, deter technological progress. We have accordingly written the final rule to frame the standard in terms that are as generic as possible and which, generally speaking, may be met through various approaches or technologies. [Preamble – Federal Register, Volume 68, No. 34, Page 8336.]

Risk Analysis Requirements

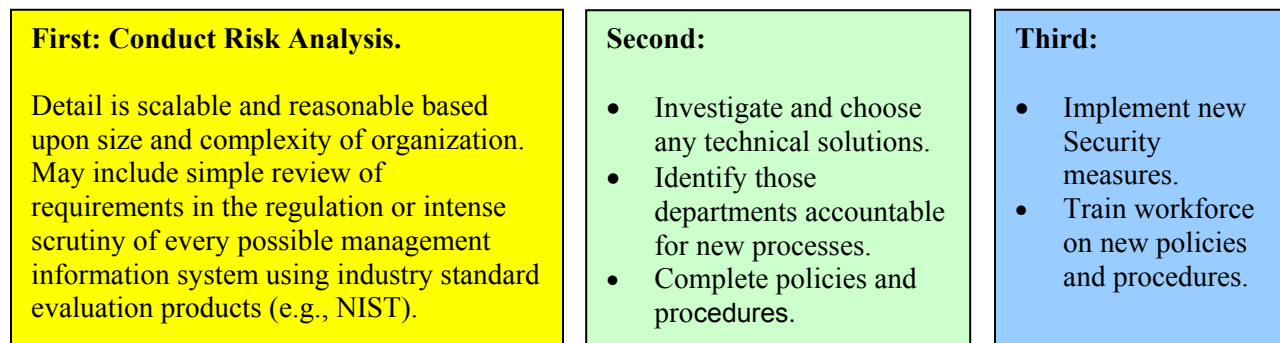
Risk analysis is defined in the final Security Rule as follows: "Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

This requirement is very clear: Each covered entity must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information (ePHI). The Security Rule does not require a covered entity to perform a risk analysis with respect to paper and oral PHI: the Security Rule only applies to ePHI. However, it is important to keep in mind that § 164.530(c) of the final Privacy Rule requires that each "covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.... 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.” In other words, while WEDI SNIP recognizes that *the Security Rule applies only to ePHI, the Privacy Rule applies to all PHI. Accordingly, it is recommended by WEDI that the risk analysis address paper-based and oral PHI as well as ePHI.*

Timing: The risk analysis should be conducted before completing security policies and procedures. Consider the following Preamble excerpt: “An entity must identify the risks to and vulnerabilities of the information in its care before it can take effective steps to eliminate or minimize those risks and vulnerabilities” (Page 8346). The risk analysis allows the organization to evaluate areas of risk, prioritize the work effort and allow time for investigation, selection and implementation of any necessary technical solutions all in time to train the workforce before the HIPAA compliance deadline. The risk analysis will help identify existing policies and procedures that need to be documented and others that need to be modified to comply with the HIPAA requirements.

Consider the following timeline for initial implementation:



Once this process is completed, keep in mind that security measures must remain current. Some form of ongoing risk analysis must be repeated as necessary in order to allow for the organization’s adopted measures to be effective and current as the organization’s security environment changes over time.

How to Approach the Risk Analysis Process

This white paper provides guidance on how to conduct a risk analysis. It addresses each of the Security Rule requirements and discusses the kinds of issues that each covered entity must consider. The white paper also provides examples of how the approach to the risk analysis will vary among different kinds of covered entities with different levels of sophistication, technology, and resources.

Assemble Your Team: As with privacy, security must be implemented with a cross representation of expertise. If the organization is large enough to have multiple operational departments, the risk analysis team should be multi-departmental. The team should include those most familiar with the organization’s electronic systems (Security Officer and information technology staff) and also should include those responsible for compliance, the Privacy Officer, regulatory/legal representation, those responsible for operations, a senior level official responsible for overall compliance who has ability to focus staff and budget, and those who will have ongoing responsibility for training and for ownership of each policy and procedure. Of course, smaller organizations may have significantly smaller teams.

The Process: First you need to understand the Security Rule requirements. Read the rule and the preamble.

Understand the community environment. If possible, work with peers from other organizations to understand how they will be implementing Security Rule requirements. This will allow you to judge the security process you will implement as compared to the standard community practice for organizations of your type and size.

Understand your unique security environment: Get or develop a schematic of your system configuration. Talk with your information technology people about how your system is set up versus how it is capable of being used. Discuss recent security incidents that may have compromised data confidentiality, integrity, and availability. Discuss security topics at a high level as defined in the rule. Start with the security requirements chart from the Security Rule (see Appendix A).

Identify, evaluate and document your “assets” in order to define what you need to develop procedures to protect. An asset is what the organization values and wishes to protect in order to stay in business. Assets can be defined in terms of quantity and quality – and exact values can be documented. Assets may include: electronic confidential information; the organization’s reputation; other forms of data (e.g., financial); computer hardware and software; buildings and real estate; and workforce members.

Identify possible threats to those assets (and the associated risk level of each threat). A threat is defined as “the potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.” Consider threats to those assets in the form of related losses as well. A threat can be a computer or other process, an activity or an event. Consider the expected frequency of possible threats as well as the “level of criticality,” i.e., how serious the damage would be to the organization if the threat were carried out.

Consider natural threats like fires, earthquakes, floods, thunderstorms, and hurricanes. Consider accidental threats like contamination and those that are created by humans, including malicious threats like bombs, terrorist activities, theft, and vandalism. Losses can be categorized in different ways:

- direct loss of lives and business operations (e.g., as a result of natural disaster or terrorist activities);
- delays or denials of services (e.g., due to computer virus);
- loss of reputation (e.g., due to inappropriate disclosure of confidential information); and
- data alteration or destruction (loss of integrity).

Losses can be direct (cost to replace computer) and indirect (cost of personnel to work overtime to fix a computer virus problem and make up the interruption of business operations). Indirect costs can also be “intangible,” e.g., the cost of embarrassment or loss of reputation.

Two final things should be considered. First, document every step of the risk analysis. Should there be a problem resulting in a security breach, this documentation will help to demonstrate that you did the risk analysis and reasonably identified your risks and threats.

Second, you will need to determine the depth of review necessary for your organization. If your organization is complex, you may need to conduct a more in depth risk analysis on certain business lines and/or entire information systems. Consider whether industry guidelines, such as NIST, ISO 17799, or others, should be used. A small, non-complex covered entity such as a small practice may simply “start with the chart” (see Appendix A) and use it as a high level risk analysis outline. Of course, a basic review of the small practices assets, potential threats and related losses needs to be completed and will assist in the decision on any changes necessary to meet the Security Rule requirements.

Goal of Risk Analysis: The goal of the risk analysis is to provide the information needed to make risk management decisions that are informed, documentable, and supportable regarding the degree of security

remediation that the organization needs to undertake to meet the requirements of the Security Rule. A more comprehensive and higher quality risk analysis is expected to lead to better and more cost effective risk management decisions. If the risk analysis only defines the areas of concern and documents identifying those areas, it will be more difficult to make cost effective and supportable risk management decisions.

The information needed to make informed risk management decisions includes identifying gap or deficiency in each of the following three items:

- level of threat: the likelihood of an incident occurring;
- impact: the effect a particular incident would have (this could be ranges and include direct costs, legal liability, and loss of reputation or goodwill); and
- counter measure options and costs: what options have been considered for mitigating the risk and the cost of those options.

Specific Security Rule Requirements

The remainder of this white paper covers the specific requirements in the final Security Rule, addresses the HIPAA security requirements in the Privacy Rule, and offers some suggestions for covered entities to consider when designing their approach to risk analysis for each of these requirements. Again, it is recognized that the Security Rule allows for flexibility in strategic design and process. The regulations provide the rules, but the covered entities must choose the appropriate technical and policy solutions. Additional information with respect to small organizations can be found in the “Small Practice Security Implementation White Paper” on the Security and Privacy Workgroup portion of the WEDI/SNIP Web site – snip.wedi.org.

Standards and Implementation Specifications

It is important to understand the specific requirements of the Security Rule and how each provision should be addressed. The rule provides a number of “standards” and “implementation specifications.” These are divided into three categories: administrative safeguards, physical safeguards, and technical safeguards.

A “standard” is a general requirement that must be complied with by the covered entity. An example of a standard is “contingency planning.” It states organizations must have contingency plans in case of emergencies or disasters. This is a general requirement.

An “implementation specification” is a more detailed and specific description of the method or approach that a covered entity can use to meet a particular standard. For example, under contingency planning, there are five implementation specifications that provide specific direction on how to proceed. These include a data back up plan, disaster recovery plan, emergency mode operation plan, testing and revision procedures, and applications and data criticality analysis. Not all standards have implementation specifications.

In addition, covered entities must adopt certain organizational requirements, such as business associate contracts, that are very similar to the business associate agreements required by the HIPAA Privacy Rule. Furthermore, a covered entity must adopt certain policies and procedures, including documentation requirements, to comply with the Security Rule.

“Required” and “Addressable”

Some implementation specifications are “required” and some are “addressable.” If an implementation specification is “required,” then the covered entity must take action to implement the specification. If it is “addressable,” then the covered entity does not need to take action to implement the specification. However, in reviewing addressable implementation specifications, a covered entity must:

- assess whether the specification is a reasonable and appropriate safeguard for the covered entity;
- implement the specification if reasonable and appropriate; or
- if implementing the specification would not be reasonable and appropriate, document this fact, and implement “an equivalent alternative measure” if reasonable and appropriate.

HHS has stated that a covered entity also may decide that a particular implementation specification does not apply to its organization and that the particular standard can be met without implementing an alternative measure in place of the addressable implementation specification. The covered entity must document such decisions and the rationale behind such decisions.

It is strongly recommended that the full risk analysis be conducted against each requirement before deciding if one element is addressable and not reasonable and appropriate. In other words, one must consider the level of threats and potential risks to electronic information and other forms of PHI before deciding if the element does not need to be addressed. As is stated above, if the final decision is not to implement (or to implement an alternative solution), the decision making process should be well documented.

“REMEMBER: Addressable” does not mean “optional.”

Administrative Safeguards¹

The administrative safeguards relate to the administrative actions the covered entity must consider during the risk analysis process in order to implement the Security Rule. These safeguards primarily relate to the “workforce” and the way the covered entity trains and expects its staff to carry out the security requirements. The administrative safeguards concern policies, procedures, and processes and support physical and technical security. (Physical and technical security are covered later in this white paper.) The risk analysis should provide a solid documentation trail of the current practices and shortcomings identified with respect to these practices.

The administrative safeguards contain a number of standards. Under several of the standards are implementation specifications:

- **Security Management Process:** risk analysis, risk management, sanction policy, and information system activity review;
- **Assigned Security Responsibility;**
- **Workforce Security:** authorization and/or supervision, workforce clearance procedure, and termination procedures;
- **Information Access Management:** isolating health care clearinghouse function, access authorization, and access establishment and modification;
- **Security Awareness and Training:** security reminders, protection from malicious software, log-in monitoring, and password management;
- **Security Incident Procedures:** response and reporting;

¹ § 164.308.

- **Contingency Plan:** data backup plan, disaster recovery plan, emergency mode operation plan, testing and revision procedures, and applications and data criticality analysis;
- **Evaluation;** and
- **Business Associate Contract and Other Arrangement:** written contract or other arrangement.

Each of these nine areas with 21 implementation specifications is addressed in the following sections of the white paper. The white paper focuses on risk analysis considerations in each of these areas. It also addresses both ePHI – as covered under the Security Rule – and paper-based and oral PHI – as covered under the Privacy Rule. It is necessary to take “reasonable” steps to protect all PHI, and a good way to ensure all PHI is reasonably protected is to address the Security of paper-based and oral PHI as part of an overall HIPAA risk analysis.

Standard: Security Management Process²

Implement policies and procedures to prevent, detect, contain, and correct security violations.

The first standard requires covered entities to implement a security management process. A key to compliance is complete and current documentation of all security measures in effect. Documentation, such as an office policy and procedure manual, should include contingency plans, formal records processing and procedures, information access controls, security incident procedures, awareness and training, and all other security aspects addressed by the Security Rule. A covered entity’s policies and procedures should become required reading by employees and always available for reference.

Your risk analysis should document current processes. It should note whether additional work is needed by the organization, e.g., development of a complete set of policies and procedures to address the Security Rule requirements. The status of your current procedures and adherence with the Security Rule requirements is addressed in the remainder of this white paper.

Implementation Specification: Risk Analysis (Required)

HIPAA Standard: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

This white paper offers examples of how an organization can work towards meeting this requirement.

Implementation Specification: Risk Management (Required)

HIPAA Implementation Specification: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).

Risk management is the process of furthering the risk analysis process by taking steps to reduce risk to an acceptable level and maintaining an acceptable level of risk over time. The risk analysis assesses the current level of risk and should help determine what is an acceptable level of risk for the covered entity. Risk management involves: (1) how to reduce unacceptable risks to reasonable levels; and (2) how to maintain that lower acceptable level of risk over time. Keep in mind that risks change over time. For example, anti-virus computer programs and “firewalls” to prevent inappropriate access to computers from outside sources must be updated on a regular basis to ensure an acceptable level of risk. Accordingly, risk management is an ongoing process.

² § 164.308(a)(1)(i).

WEDI SNIP suggests that your risk analysis might address the following questions:

- How does the organization currently manage its security risks? Is this appropriate and reasonable?
- What does the organization do to ensure risks remain at reasonable levels over time? If not much is being done, or if what is being done is not adequate and reasonable, it may be necessary to identify current risk management shortcomings.
- Do risk management policies and procedures adequately protect confidential information? If not, identify the issues that need to be addressed.
- Who in the organization is accepting “mitigated” or “unmitigated” risk? Is this level of management appropriate for the level of risk being accepted?

Implementation Specification: Sanction Policy (Required)

HIPAA Implementation Specification: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

A security sanction policy should serve to reinforce the covered entity’s security policies and procedures. The sanction policy should be a clear statement of the consequences to a member of the covered entity’s workforce of not adhering to all the policies and procedures. Recall that sanctions are a required component of Privacy Rule implementation.

WEDI SNIP suggests that your risk analysis might address the following questions:

- Do the current privacy sanction policies and procedures apply to security breaches related to ePHI, paper-based PHI, and oral PHI? If not, it will have to be expanded.
- Do the sanction policies address varying degrees of disciplinary action? Various sanctions up to and including termination should be included.
- Do the sanction policies apply to all workforce members, including management? The sanction policies must apply to **all** workforce members.
- Do the sanction policies address contractors, consultants, etc.? Everyone with access to PHI should be covered by the policy.
- Is it necessary to change current sanction policies and procedures to incorporate security breaches?
- Are the current sanctions reasonable or do they need to be changed? Do the sanctions fit with the harm or potential harm associated with various security breaches?
- Are the current sanctions enforced as a standard (and not intermittently)? Sanctions must be applied in a uniform fashion.

Implementation Specification: Information System Activity Review (Required)

HIPAA Implementation Specification: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

The covered entity needs to review all information system activity logs, reports, and incident reports. These log and reports are discussed elsewhere in the rule, e.g., log-on monitoring and audit controls. It is not sufficient to simply collect the information. The organization must also review the information to identify security problems that need attention.

WEDI SNIP suggests that your risk analysis address the following questions:

- Is there a process to routinely review information system activity logs and reports, manual and/or automated? If not, you will have to develop such a process.
- Does the organization develop corrective action plans, as appropriate, to address any security issues identified through such reviews? You will have to ensure appropriate follow up for all identified security issues.
- Does the policy address how long audit logs, access reports and security incident tracking reports are retained? Documentation and retention should be addressed.

Standard: Assigned Security Responsibility³

HIPAA Standard: Identify the security official who is responsible for the development and implementation of the policies and procedures required by [the Security Rule] for the entity.

Covered entities are required to designate one person as the Security Official who will be responsible for developing and implementing the organization's security policies and procedures. This mandate is similar to the requirement under the Privacy Rule that one person to be named as the organization's Privacy Officer.

WEDI SNIP suggests that your risk analysis address the following questions:

- Is there one individual designated as the Security Official? If not, the organization will have to designate a Security Official.
- Are the Security Official's responsibilities for developing and implementing the organization's security policies and procedures clearly defined? The role and responsibilities of the Security Official need to be clearly documented.
- Is there cross-functional support for the Security Official within the organization?
- Is there clear and visible management support for the Security Official's responsibilities?
- Does the Security Official have the proper level of experience and training needed to be a Security Officer?
- How do the Security Official and Privacy Officer coordinate regarding HIPAA issues? Are their roles clear?

Standard: Workforce Security⁴

HIPAA Standard: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

There are several implementation specifications that need to be considered in this portion of a risk analysis.

Implementation Specification: Authorization and/or Supervision (Addressable)

HIPAA Implementation Specification: Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

³ § 164.308(a)(2).

⁴ § 164.308(a)(3)(i).

Authorization is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program. Authentication is proving that a user is whom s/he claims to be. Authentication and authorization go hand in hand. Based upon the results of your risk analysis, your organization may need to assure that users must be authenticated before carrying out the activity they are authorized to perform. (See also Standard: Person or Entity Authentication, page 29.)

WEDI SNIP suggests consideration of the following, which address the requirements in the Privacy Rule as well as in the Security Rule, when completing your risk analysis:

- Is there a procedure for determining which employees and groups of employees have access to specific ePHI and other PHI? If not, one will have to be implemented.
- Who manages granting, modifying (when responsibilities change), and terminating access to systems, applications, databases and directories that contain ePHI and other PHI? Is the person who responsible for authorizing access different from the person responsible for granting access to ePHI and other PHI? The roles of each individual involved in this process should be clearly defined.
- Are reasonable efforts made to identify and authenticate employees prior to their obtaining access to ePHI and other PHI? It may be necessary to change procedures to ensure this is accomplished.
- Are access authorization records maintained? Part of your HIPAA documentation should include such records.

Implementation Specification: Workforce Clearance Procedure (Addressable)

HIPAA Implementation Specification: Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

Based upon results of your risk analysis your organization may need to assure that personnel are granted access to health information only after receiving appropriate clearances. This is important to prevent unnecessary or inadvertent access to secure information. The covered entity should employ personnel clearance procedures prior to hiring. This could consist of standardized personnel and professional reference checks.

WEDI SNIP suggests your organization consider the following questions when completing the risk analysis:

- Are checks on permanent staff carried out before hiring? If not, consider implementing such checks, particularly for individuals with access to sensitive information.
- Are checks on temporary staff carried out either by contract with the temporary staffing agency or by the covered entity prior to allowing access to ePHI and other PHI? It may be necessary to change staffing agencies or alter the contract with a staffing agency to ensure this is done. [*Note:* Temporary staff includes students, staff augmentation, credentialed providers who are not employees of the organization, etc.]
- Are employees asked to sign confidentiality or non-disclosure agreements as a part of the terms and conditions of employment? This may occur in conjunction with HIPAA training.

Implementation Specification: Termination Procedures (Addressable)

HIPAA Implementation Specification: Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section [of the Security Rule].

WEDI SNIP suggests that formal documented procedures, which include appropriate security measures for the termination of an employee's employment or an internal/external user's access, should be in place. The key is to prevent the possibility of unauthorized access to confidential data by those who are no longer authorized to access the data.

WEDI SNIP suggests consideration of the following questions, which need to address ePHI as well as all other PHI:

- Is there a procedure to ensure all physical items (keys, tokens, or cards) that allow a terminated employee to access a property, building, or equipment are retrieved from that employee, preferably before termination?
- Is there a procedure for changing combinations of locking mechanisms, if appropriate, both on a recurring basis and when personnel knowledgeable of combinations no longer have a need to know or require access to the protected facility or system?
- Have all organizational assets assigned to the employee that have the capability of storing confidential data (e.g., laptop, PDA, flash drives, and cell phones) been retrieved prior to termination?
- Is physical eradication of a person's access privileges performed in a timely manner?
- Are an individual's access privileges (including remote access) to the information, services and resources for which they currently have clearance terminated or deleted in a timely manner?
- Is periodic auditing of the effectiveness of the process for disabling access performed?
- Are suspended accounts periodically monitored for activity or attempted activity?
- Are all processes as outlined above formally documented?
- Do additional processes need to be implemented?
- Is there a separate process and procedure for handling disgruntled or volatile terminations? If not, does there need to be?
- Is there a process and procedure for removing contractor/consultant access in a timely manner when their contract expires or is terminated?

Standard: Information Access Management⁵

HIPAA Standard: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of Subpart E [HIPAA Privacy Rule] of this Part.

Policies and procedures may need to be implemented to allow workforce members appropriate access to electronic protected health information.

Implementation Specification: Isolating Health care Clearinghouse Function (Required)

HIPAA Implementation Specification: If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

Some covered entities perform a variety of functions. If an entity, including a covered entity, provides clearinghouse functions within a larger organization, the ePHI of the clearinghouse must be isolated from the larger organization.

WEDI SNIP suggests that your risk analysis address the following questions:

⁵ § 164.308(a)(4).

- Does the organization provide clearinghouse functions? If not, you can ignore this implementation specification. (However, you should be sure to document the decision making process).
- Does the organization have policies and procedures to isolate clearinghouse functions from the remainder of the organization?
- Is access to the clearinghouse ePHI monitored to ensure it is isolated? Auditing is vital to document the ePHI is actually isolated. (See Standard: Audit Controls, page 28.)

Implementation Specification: Access Authorization (Addressable)

HIPAA Implementation Specification: Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

Each covered entity should consider developing and implementing policies and procedures for granting and maintaining privileges for individuals to access electronic confidential information. The Security Officer or some other individual should document and maintain such access authorization records. The covered entity should document authorization for access and level, defined time and document roles. When non-workforce personnel use the computer for maintenance or hardware installation, they need authorization, and should be required to sign and date the required documents (e.g., a confidentiality agreement).

WEDI SNIP suggests your risk analysis address the following questions:

- Does the organization grant access to ePHI for each individual within the organization based on the individual's job functions? The organization must ensure that each individual has access to only the ePHI they need to perform their jobs.
- Does the organization control access to ePHI at the workstation, program, process, or records level, as appropriate? Each organization must evaluate the appropriate level at which to control access to ePHI. The larger the organization and the more ePHI it has, the greater the likelihood that more specific controls is necessary.

Implementation Specification: Access Establishment and Modification (Addressable)

HIPAA Implementation Specification: Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Once access has been authorized, the covered entity needs to consider creating and implementing policies and procedures to establish that access and to modify that access in the future as needed. The procedures should describe how access is actually implemented through the use of various systems and procedures, including passwords and card keys. An authentication policy will establish trust through an effective password policy, and by setting guidelines for remote location authentication and the use of authentication devices (e.g., one-time passwords and the devices that generate them). An accountability policy defines the responsibilities of users, operations staff, and management. It should specify an audit capability, and provide incident handling guidelines as appropriate.

WEDI SNIP suggests your risk analysis address the following question:

- Does the organization monitor access to ePHI and modify access on an ongoing basis? The organization should monitor access to ensure individuals have access to the ePHI they need and no

more. If an individual has too little access, access should be authorized and expanded. If they have too much access, access needs to be restricted.

Keep in mind that a similar provision exists in the Privacy Rule: the minimum necessary requirement. You should ensure that your risk analysis adequately addresses the minimum necessary requirement.

Standard: Security Awareness and Training⁶

HIPAA Standards: Implement a security awareness and training program for all members of its workforce (including management).

The covered entity must consider the development of a mechanism to ensure that **all** members of its workforce, including management, are aware of security issues and are adequately trained. Security training requires education concerning the vulnerabilities of the confidential information maintained by the covered entity and the covered entity's policies and procedures to protect that confidential information. Four implementation specifications are listed under this standard.

Most covered entities are significantly at-risk for lack of awareness and training. Even though the implementation specifications are addressable, a risk analysis should carefully review this area. Studies report that administrative matters account for 70-80% of HIPAA security compliance. There are many reasonably priced products available that can address security awareness and training. It should be role-based. Accordingly, information technology personnel should receive intensive training while clinical or administrative personnel may receive less intensive awareness training. Given the short time frame for implementation, covered entities should begin the HIPAA Security training as soon as possible in order to test retention of the security-related material.

Implementation Specification: Security Reminders (Addressable)

HIPAA Implementation Specification: Periodic security updates.

Periodically reminding employees of their security responsibilities is recommended. Security reminders are effective for reinforcing what has been learned through more formal security training. Periodic security reminders should roll out on a regular basis (e.g., at least quarterly) to ensure the workforce is up to date on all security issues.

WEDI SNIP suggests your risk analysis address the following questions:

- Does the organization provide periodic security updates, related to both ePHI and other PHI? If not, do they make sense for the organization?
- What media are used and what media are best for providing the updates, e.g., e-mails, posters, memoranda, Intranet, and newsletters? The organization should consider using a variety of approaches to reinforce key security policies and procedures.
- How are security update topics be selected and by whom? Security reminders should address problem areas.
- How often are security updates provided and by whom? Make sure developing and delivering periodic reminders is assigned to appropriate staff.

⁶ § 164.308(a)(5).

- Does the organization provide periodic “refresher” training? Is this training documented? Periodic refresher courses are an effective way to make sure workforce members understand the organization’s policies and procedures address common concerns.

Implementation Specification: Protection from Malicious Software (Addressable)

HIPAA Implementation Specification: Procedures for guarding against, detecting, and reporting malicious software.

It may be obvious to most computer users that the use of non-sanctioned software or unlicensed software is a bad practice. However even the most advanced entities fall victim to this practice. The organization should consider developing a policy that clearly spells out penalties for the use of disapproved software. All employees need to be trained on this policy. In addition, it is necessary to install programs to prevent unwanted programs and software from being inadvertently installed on computers. To that end, a firewall and virus protection is recommended.

WEDI SNIP suggests your risk analysis address the following questions:

- Does the organization have virus protection and firewall programs installed? If you connect to an intranet or the Internet, or if you allow anyone to install data or software from a diskette, CD, or DVD, such programs are necessary.
- Are the programs appropriate for the organization and its system configuration? An off the shelf product may be appropriate for your environment to sufficiently lessen the degree of risk associated with receiving malicious software or you may need to implement a customized program.
- If the system configuration is a network, is anti-virus software (updates and scans) controlled at the server level (thereby assuring there is no chance an “end-user” could override or ignore an update)? Do you have appropriate safeguards at the server and workstation levels? It is important to protect all access points.
- Does the organization prevent use of non-business related software from home or any other location, including downloads? Such programs often carry malicious software.
- Are systems properly “patched” (patch management) in an expeditious manner to avoid being exploited by malicious logic that takes advantage of improperly patched systems? System updates are issued on an ongoing basis and should be installed.
- Are users periodically trained on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail? Users need to be involved in protecting systems from malicious software.

Implementation Specification: Log-in Monitoring (Addressable)

HIPAA Implementation Specification: Procedures for monitoring log in attempts and reporting discrepancies.

One key to HIPAA compliance is the ability to audit and document log in attempts. It is recommended that covered entities track all log-ins and block illicit login attempts.

WEDI SNIP suggests your risk analysis address the following questions:

- Does the organization track all system and application log-ins? Such tracking will allow the organization to know who is accessing ePHI as well as who is attempting to access ePHI.

- Does the organization review the login reports (manually or using an automated system) to identify potential security problems? Are potential problems addressed? Incidents should be identified and corrective action taken as appropriate.

Implementation Specification: Password Management (Addressable)

HIPAA Implementation Specification: Procedures for creating, changing, and safeguarding passwords.

Each covered entity should consider development of a policy and training mechanism to assure that every employee understands they are responsible for their password, the facility's policies and procedures regarding passwords, and the ramifications if they give out a password. New employees should be given an overview at orientation of the general dos and don'ts, e.g., don't tape your password to your computer or share with others for any purpose. This may occur as part of HIPAA training. In addition, passwords should not be easily guessed. Two recommendations include not allowing dictionary or common names, and forcing users to use a combination of number and letters. Passwords should be as difficult as possible, but not so difficult that staff cannot remember them.

WEDI SNIP suggests your risk analysis address the following questions:

- Do you have an effective password management program? If you are not sure, additional work may be needed.
- Are workforce members required to change passwords on a regular basis, e.g., every 60 or 90 days? The shorter the better from a security perspective (as long as workforce members can remember the passwords).
- Are workforce members required to use passwords that are not easily guessed, e.g., no names and passwords that include letters and digits? The more complex the passwords, the greater the security (as long as workforce members can remember the passwords).
- Are workforce members trained to understand the appropriate use of passwords and the need to keep passwords private? Consider making this part of HIPAA training.

Standard: Security Incident Procedures⁷

HIPAA Standard: Implement policies and procedures to address security incidents.

Covered entities have to implement policies and procedures for handling and documenting "security incidents" and their resolution. A security incident is defined as an "attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system."

Implementation Specification: Response and Reporting (Required)

HIPAA Implementation Specification: Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

Covered entities are required to identify and respond to suspected or known security incidents; mitigate damages resulting from known security incidents, if possible; and document security incidents and their

⁷ § 164.308(a)(6).

outcomes. The covered entity must document procedures to identify security incidents, procedures to report those incidents, and procedures to respond to incidents, as appropriate.

Before any analysis can be conducted to determine the scope of what should be accomplished to comply with this standard, one must first define what a security incident is and is not. In the comment section of the Security Rule it states:

Whether a specific action would be considered a security incident, the specific process of documenting incidents, what information should be contained in the documentation, and what the appropriate response should be, will be dependent upon an entity's environment and the information involved. An entity should be able to rely upon the information gathered in complying with other security standards, for example, its risk assessment and risk management procedures and the privacy standards, to determine what constitutes a security incident in the context of its business operations.

§164.304 defines a security incident as “the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.” §164.304 further defines system as “an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people.”

Generally, an incident is any event that may compromise the security of a system (operating system, application, database, etc.), a network, or data. An incident need not be real; even the threat of such an event can be considered an incident in many cases. The term “security incident” can include a broad range of topics. Some examples of incidents are: property theft (hardware or software); compromised passwords, tokens, or other means of controlled access to PHI; lost access badge; unauthorized access (physical or logical); unauthorized disclosure of PHI (hardcopy or electronic); unauthorized use of accounts or privileges; tampering with data with malicious intent; misusing PHI; malicious code or virus; hoaxes that cause stress and waste of business resources; hacking (actual or attempted); criminal activity; identity theft; fraud; improper network activity (e.g., probes or network mapping from unknown or unauthorized sources); and denial of service attacks or attempts. Incidents can also be accidental or natural, for example: electrical power outages; hardware failures; human error; and acts of God (e.g., tornados, fire, earthquake, and hurricanes.)

WEDI SNIP suggests your risk analysis address the following questions:

- Does the organization have a definition of “security incidents”? Does it meet the requirements of the Security Rule? It may be necessary to redefine what is considered a security incident.
- Are processes or systems in place to identify all security incidents and the impact of those incidents? If not, new processes or systems will need to be implemented.
- Has an emergency communications plan been developed to address how, when and to whom security incidents will be reported? Has someone been appointed to be the primary focal point for all security incidents? Your risk analysis will need to determine not only who this should be, but if there is a need for it to be more than one person. Be sure to address internal and external communications.
- Are processes or systems in place to contain and eradicate problems resulting from security incidents? If not, processes or systems will need to be implemented.
- Does the organization have processes in place to recover from security incidents? Procedures may need to be revised and implemented. Procedures addressing restoration, validation and monitoring of systems impacted by an incident all need to be addressed in your procedures. (See Standard: Contingency Plan, page 17.)

- Are security incidents and the outcome of each incident tracked? Here again, documentation is necessary to show compliance with HIPAA.
- Does the organization have a process to learn from security incidents and to alter systems and processes to minimize the impact of future incidents? Incidents should be fed into an ongoing risk analysis/evaluation and security changes implemented as appropriate.

Standard: Contingency Plan⁸

HIPAA Standard: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

Your risk analysis must include a review of assets and related threats in enough depth to allow for high level planning in the event of a negative occurrence that may be man-made, natural or environmental. It must include the definition of basic emergency contact information for each necessary workforce member, critical business partners and others required to assure successful business and data restoration. It should allow for this critical contact information to be retrieved (whether electronic files or paper lists of contact names) from the business site as well as an alternative site (preferably located in a separate geographic location).

The first three-implementation specifications under this specification are required and the last two addressable.

Implementation Specification: Data Backup Plan (Required)

HIPAA Implementation Specification: Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

Each covered entity must backup PHI and store it appropriately. It is important to keep a copy of the backup at an alternative site data in case the site is destroyed. Remember that the backup must be kept in a secure location.

WEDI SNIP suggests your risk analysis address the following questions:

- Has all of the ePHI in the organization's systems been identified? This is the first step in backing up data and should be addressed in a PHI inventory.
- Is there a defined documented process outlining how staff perform the backup and validate its content (integrity of data)? A written procedure is necessary to ensure the organization has a complete and appropriate process.
- Is the backup performed on a regular basis? Each organization will have to determine what is reasonable. In most organizations it is likely that daily will be considered reasonable.
- Does the organization perform routine testing of use of the backup media to assure the process and media is in working condition? It is important to verify data actually can be restored from the backups.
- Is backup information stored off the premises of the organization, preferably in a separate geographic location? If not, consider such storage. Make sure the offsite storage is secure.

⁸ § 164.308(a)(7).

Implementation Specification: Disaster Recovery Plan (Required)

HIPAA Implementation Specification: Establish (and implement as needed) procedures to restore any loss of data.

It is vital to have procedures to restore any lost or altered electronic protected health information when such electronic protected health information's integrity has been compromised due to a negative event.

WEDI SNIP suggests your risk analysis address the following questions:

- Has the organization identified those staff responsible to carry out data restoration, including lists of emergency contact names and numbers, important business partners as well as potentially hardware, software and other business supply contact information as would be necessary to allow for a temporary office set-up to support complete restoration of data in order to continue business functioning? Make sure vital information is available offsite in case the site is inaccessible.
- Has the organization performed detailed testing and revision of its plan? Plans may need to be updated and changed on an ongoing basis.

Implementation Specification: Emergency Mode Operation Plan (Required)

HIPAA Implementation Specification: Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

Each covered entity must determine what systems need to be in operation and how quickly those systems need to be in operation following a security event. This will vary widely. In a small practice with minimal ePHI, it may be acceptable to be without computers and restored systems for a few days. In a hospital, it may be unacceptable to be without data systems in the ICU for more than a few minutes.

WEDI SNIP suggests your risk analysis address the following questions:

- Has the organization identified those critical business processes that must occur in order for the organization to continue operations during and immediately after a crisis situation? This will help to focus resources on the most important systems first.
- Has the organizations made reasonable and appropriate arrangements to ensure that its critical business processes can be up and running in an appropriate time frame? This may include having an offsite location ready for operation, mirroring data at a remote site, having agreements with suppliers to rapidly provide equipment, and having an uninterruptible power supply.

Implementation Specification: Testing and Revision Procedure (Addressable)

HIPAA Implementation Specification: Implement procedures for periodic testing and revision of contingency plans.

Often, simple steps in conducting disaster recovery or other business continuity planning revival are missed because they have not been tested from start to finish. While implementing a testing and revision procedure or process is considered addressable, it is worthwhile to periodically prepare a "test run." Human emotions and inability to think clearly during a crisis situation alone drive the need to routinely test and revise procedures to assure that even staff unfamiliar with the process can follow step by step instructions to facilitate continuity of the business during and immediately after a crisis.

WEDI SNIP suggests your risk analysis address the following questions:

- Has the organization tested its plan? Testing the plan will help the organization determine how it will work in a crisis. In addition, testing helps train personnel.
- Has the organization evaluated the results of the test and revised its plan as appropriate? It is not enough simply to perform a test. The organization should strive to learn from the test and revise its plan as needed.
- Does the testing occur on a routine basis? Over time personnel, systems and system configurations, and the security environment change. As such, ongoing testing is important.

Implementation Specification: Applications and Data Criticality Analysis (Addressable)

HIPAA Implementation Specification: Assess the relative criticality of specific applications and data in support of other contingency plan components.

Your organization should consider implementing a process to review the various computer and other electronic systems critical to the organization. Applications and data criticality analysis allows for a prioritization or ordering of the various systems. This allows for resources to focus on those systems and support processes most critical to the business first, should staff resources or ability be diminished due to a disaster or other negative event.

WEDI SNIP suggests your risk analysis address the following question:

- Has the organization evaluated its systems and ranked them in order of importance to the ongoing operation of the organization? This analysis will help in developing the contingency plan and focusing resources in an emergency.

Standard: Evaluation⁹

HIPAA Standard: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this [Security Rule].

This has been discussed in several sections above. Once the security policies and procedures are implemented with an appropriate level of risk of that security being breached, the covered entity cannot simply sit back. As the environment changes, risks change.

WEDI SNIP suggests your risk analysis address the following questions:

- How does your organization evaluate the changing security environment? As discussed in other sections of this white paper, the organization should be tracking security issues and compliance. This information should be used to evaluate evolving and new threats and risk levels.
- Does your organization plan to perform ongoing risk analyses on a periodic basis? It is necessary to periodically ensure the organization is still meeting the security requirements within a changing security environment. Consider whether it is appropriate to periodically be evaluated by a neutral, disinterested third party.

⁹ § 164.308(a)(8).

Standard: Business Associate Contracts and Other Arrangement¹⁰

HIPAA Standard: *A covered entity, in accordance with 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the associate will appropriately safeguard the information.*

Both the Privacy Rule and Security Rule require covered entities to enter into Business Associate Agreements or Contracts with certain outside parties that have access to the covered entity's ePHI. **Note:** The Security Rule does not extend the length of time (as did the Privacy Rule) allowed for Business Associate Agreements to be completed past the official compliance date.

Implementation Specification: Written Contract or Other Arrangement (Required)

HIPAA Implementation Specification: *Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate the meets the applicable requirements of Section 164.314(a).*

The Security Rule does contain an additional requirement for the agreement to require the Business Associate to notify the covered entity if the Business Associate becomes aware of a "security incident." Also, the Security Rule makes it clear that Business Associates must implement "administrative, physical and technical safeguards" to protect electronic confidential information, and must require subcontractors to implement "reasonable and appropriate" safeguards to protect electronic confidential information.

WEDI SNIP suggests your risk analysis address the following questions:

- Have all Business Associates that have access to ePHI and other PHI been identified? This should have been completed as part of Privacy Rule implementation.
- Has justification for such access been documented? This also should have been completed as part of Privacy Rule implementation.
- Is there a signed Business Associate agreement with each Business Associate that has access to ePHI? This also should have been completed as part of Privacy Rule implementation; however, language specifically pertaining to the requirements of the Security Rule may need to be added.
- Does the agreement require the Business Associate to implement and maintain administrative, physical and technical safeguards? Does the agreement require the Business Associate to ensure subcontractors implement reasonable and appropriate safeguards to protect the Covered Entity's ePHI? While this was required by the Privacy Rule, the organization may want to better define what is required given the specification of the Security Rule.
- Does the agreement define "security incidents" and does it specify security incident reporting procedures? This should mirror the organization's definition (see Standard: Security Incident Procedures, page 15).

¹⁰ § 164.308(b)(1).

Physical Safeguards¹¹

The physical safeguards relate to physical actions the covered entity should consider undertaking to implement the Security Rule. The physical safeguards concern how to ensure that only appropriate individuals have physical access to facilities and electronic confidential information.

The physical safeguards contain a number of standards and several implementation specifications:

- **Facility Access Controls:** contingency operations, facility security plan, access control and validation procedures, and maintenance records;
- **Workstation Use;**
- **Workstation Security;** and
- **Device and Media Controls:** disposal, media re-use, accountability, and data backup and storage.

Each of these four areas with eight implementation specifications is addressed in the following sections of the white paper. It also addresses both ePHI – as covered under the Security Rule – and paper-based and oral PHI – as covered under the Privacy Rule. It is necessary to take “reasonable” steps to protect all PHI, and a good way to ensure all PHI is reasonably protected is to address the Security of paper-based and oral PHI as part of an overall HIPAA risk analysis.

Standard: Facility Access Controls¹²

HIPAA Standard: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

The covered entity must develop and use procedures for securing physical access to its site, e.g., locking doors, computers and storage areas. There are several implementation specifications under this standard.

Implementation Specification: Contingency Operations (Addressable)

HIPAA Implementation Specification: Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

This is an addressable implementation specification; however, all covered entities should consider having in place a plan to recover from a disaster and, if appropriate, to operate in emergency mode. This requires having appropriate backups – both data and hardware – and understanding what the most critical operations in the organization are. In some organizations it may be imperative to keep some systems running regardless of the problem, e.g., the critical care unit and operating rooms in a hospital. Other organizations may determine that it is acceptable to be “down” for a few days, e.g., most of the functions in a health plan are not time critical.

WEDI SNIP suggests your risk analysis address the following questions related to physical access to facilities under the contingency plan:

¹¹ § 164.310.

¹² § 164.310(a)(1).

- Is there a plan to get appropriate personnel onsite to restore operations in a timely fashion? This also should be part of your contingency plan (see page 17).
- Have these personnel been trained in disaster recovery and do they understand the priorities? See Implementation Specification: Disaster Recovery Plan (Required), page 18.

Implementation Specification: Facility Security Plan (Addressable)

HIPAA Implementation Specification: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

The covered entity needs to consider implementing a process to assess the overall physical security needs of the covered entity, including facility location, layout, design, and construction. For a small organization, e.g., solo practice physician office, this may be straightforward and involve simply locking the doors when no workforce member is in the office. In a large organization, this can be a complex task, especially if the facility is open to the public around the clock, e.g., a hospital.

WEDI SNIP suggests your risk analysis address the following questions:

- Does your organization have a current facility security plan? Is it up to date with your current facility design? If not, you will need to develop or update the plan.
- Does the plan cover who can access each portion of the facility (facilities)? Does access vary depending on circumstances, e.g., does it change during emergency mode operations? See also Implementation Specification: Authorization and/or Supervision (Addressable), page 9, and Implementation Specification: Emergency Mode Operation Plan (Required), page 18.
- Does the plan discuss how equipment is protected, including who can access each machine? See also Implementation Specification: Authorization and/or Supervision (Addressable), page 9, and Standard: Device and Media Controls, page 24.
 - Is it up to date and consistent with your equipment inventory?
 - Does it address all equipment, including PDAs, cellphones, and medical equipment?
- Does the plan adequately address access to paper-based PHI? Recall that the Privacy Rule requires you to keep paper-based PHI secure.
- Is the plan reviewed and updated on a regular basis? This should be part of your ongoing risk analysis (see page 7).

Implementation Specification: Access Control and Validation Procedures (Addressable)

HIPAA Implementation Specification: Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

Consider limiting physical access to appropriately authorized individuals. In a small organization, it is likely that all workforce members need access to all portions of the facility and, very likely, PHI – that is both paper and electronic. In a larger organization, job functions will be more specialized and offices physically separated. In such an organization it is important to ensure that workforce members' access is limited. These limitations should focus on keeping PHI secure. Workforce members should be granted limited access to locations that have PHI on an as needed basis. Workforce members also should be granted access to software and ePHI on an as needed basis. Access may be controlled using tokens, card keys, biometrics, and passwords, among other approaches.

WEDI SNIP suggests your risk analysis should the following questions:

- Has the organization made a determination of which job functions need access to each part of the facility and to each software program and related ePHI? Controlling physical access to portions of the facility will help to prevent inappropriate access to PHI – both ePHI and other PHI. See also Implementation Specification: Authorization and/or Supervision (Addressable), page 9.
- Are appropriate and adequate approaches used to limit physical access within the organization? The organization should evaluate access on an ongoing basis.
- How are visitors handled, including maintenance personnel, consultants, and other contractors? Temporary access and monitoring access for such individuals can be a complex issue for a larger organization with a great deal of public access.

Implementation Specification: Maintenance Records (Addressable)

HIPAA Implementation Specification: Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Maintenance records serve two purposes. First, the records indicate who accessed various portions of the facility and/or various hardware and software systems. It is important to consider monitoring such access and ensuring that it is appropriate. Second, the records indicate changes and modifications to the physical facility and hardware that may require changes or updates to the various documentation required by the rule.

WEDI SNIP suggests your risk analysis address the following questions:

- Are logs maintained of the repairs and modifications to the physical facility that may have an impact on security? The log also should record who performed the work and what access they were granted for purposes of the work.
- Are the logs reviewed to ensure the access to systems was appropriate and to verify that the changes were made in an appropriate fashion? This is necessary to ensure ongoing security.
- Are the logs reviewed to ensure that any necessary changes to the organization’s security procedures resulting from the repairs or modifications are made? This should part of the ongoing risk analysis.

Standards: Workstation Use¹³ and Workstation Security¹⁴

HIPAA Standard: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

HIPAA Standard: Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

These two standards are closely related. It is important that each covered entity have physical safeguards to protect access to workstations. Entities also need to restrict access to ePHI on each workstation based on the functions associated with that workstation. Ideally, workstations used to access ePHI should be located only in controlled areas. In some organizations this may be easy, e.g., a health plan where there is limited and controlled public access to the facility. In other organizations this may be difficult, e.g., in a hospital with public access to many areas of the facility. Keep in mind that even if an unauthorized person gains access to a

¹³ § 164.310(b).

¹⁴ § 164.310(c).

workstation, the covered entity should have appropriate technical security – authentication – to prevent the individual from actually accessing the ePHI (see page 26).

Each organization needs to develop and implement policies and procedures to protect access to workstations. These policies and procedures will be based in large part on other standards and implementation specifications, e.g., access authorization (page 9), access control (page 21), and person authentication (page 29),

WEDI SNIP suggests your risk analysis address the following questions:

- Are your workstations with access to ePHI located in controlled areas? If not, can they be moved to controlled areas?
- Are computer monitors that display ePHI properly positioned to avoid inadvertent or unauthorized viewing? Has the use of “privacy” screens been considered?
- Have you documented your policies and procedures related to workstation use and are they consistent with the Security Rule? If not, they need to be updated.

Standard: Device and Media Controls¹⁵

HIPAA Standard: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

Each covered entity is required to have in place a number of procedures to track and control devices and various media.

Implementation Specification: Disposal (Required)

HIPAA Implementation Specification: Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

Each covered entity must ensure that electronic media are disposed of appropriately. Organizations should catalog all of the locations in which ePHI is retained. This includes all devices – workstations, laptops, PDAs, cell phones, medical devices, etc. – and all media – diskettes, CDs, DVDs, etc. All of the ePHI on all of these devices and media must be destroyed when they are no longer needed.

WEDI SNIP suggests your risk analysis address the following questions:

- Have you identified the locations of all ePHI maintained by the covered entity, including temporary locations, e.g., a server through which ePHI passes? You should inventory the locations of ePHI.
- Do you have methods for destroying the ePHI from each of these locations?
 - You may need a different approach or methodology to each type of media and each type of device.
 - Keep in mind that simple solutions may work just fine, e.g., scratching a diskette with a nail and snapping it in half.
 - Also keep in mind that simply deleting a file does not destroy the information.
- Have you verified that your methodology works and that the ePHI is not recoverable? Double check that the ePHI is actually destroyed.

¹⁵ § 164.310(d)(1).

- If commercial software is being used to degauss (erase) ePHI, has the software been “certified” by recognized authority in destruction of electronic data?
- If workforce members are allowed to process ePHI on personally owned computers, have they been trained on how to properly dispose of ePHI? This may be a particular problem for some covered entities.

Implementation Specification: Media Re-use (Required)

HIPAA Implementation Specification: Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

Each covered entity needs to clean ePHI from all media prior to re-using the media. Many of the same approaches used in disposing of media can also be used to clean media prior to re-use. Keep in mind that it may be acceptable to clean and re-use media within the covered entity; however, careful consideration should be given to whether or not media will be cleaned and then re-used outside the organization. It is probably better simply to destroy the media.

WEDI SNIP suggests your risk analysis address the following questions:

- Are electronic media re-used? If so, the organization needs a written policy regarding when and how such media are reused.
- Is there a documented methodology to clean media prior to re-use? It may be necessary to obtain new software or hardware to clean the media.
- Have you tested the media to ensure that the methodology is adequate and clean and that ePHI is not recoverable? Double check that the ePHI is actually destroyed.

Implementation Specification: Accountability (Addressable)

HIPAA Implementation Specification: Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

In order to control access to ePHI, it is necessary to consider documenting the location of the information. Toward that end, it is recommended that each covered entity create an inventory of hardware and electronic media containing ePHI, including mobile devices such as PDAs and cellphones. That inventory should detail the location of and the person responsible for the hardware and electronic media. The inventory should be updated when the location or person changes.

WEDI SNIP suggests your risk analysis address the following questions:

- Does the organization have an inventory of all hardware and electronic media containing ePHI?
- Does the inventory indicate the location of and person responsible for the hardware and media?
- Is the log kept up to date, such that the movements and current locations of the hardware and media are recorded?

Implementation Specification: Data Backup and Storage (Addressable)

HIPAA Implementation Specification: Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Several sections of the rule address the need for backing up data, e.g., in connection with disaster recovery (see page 17). When equipment is moved, you should consider a process to be prepared for problems and, prior to such movement, should ensure a current backup is made of the information on that equipment.

WEDI SNIP suggests your risk analysis address the following question:

- Is a backup made of all data on equipment prior to moving the equipment? If not, the organization should update its policies and procedures.

Technical Safeguards¹⁶

The technical safeguards relate to technical items the covered entity must implement to meet the requirements of the Security Rule. The technical safeguards concern how to ensure that only appropriate individuals have electronic confidential information.

The technical safeguards contain a number of standards and several implementation specifications:

- **Access Control:** unique user identification, emergency access procedure, automatic log-off, and encryption and decryption;
- **Audit Controls;**
- **Integrity:** mechanism to authenticate electronic protected health information;
- **Person or Entity Authentication;** and
- **Transmission Security:** integrity controls and encryption.

Each of these five areas with six implementation specifications is addressed in the following sections of the white paper. It also addresses both ePHI – as covered under the Security Rule – and paper-based and oral PHI – as covered under the Privacy Rule. It is necessary to take “reasonable” steps to protect all PHI, and a good way to ensure all PHI is reasonably protected is to address the Security of paper-based and oral PHI as part of an overall HIPAA risk analysis.

Standard: Access Control¹⁷

HIPAA Standard: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4) [of the Security Rule].

This requirement also relates to the Administrative Safeguards on access authorization and access establishment and modification (see pages 12 and 15). It provides that the covered entity must implement appropriate technical safeguards to ensure appropriate access control.

Implementation Specification: Unique User Identification (Required)

HIPAA Implementation Specification: Assign a unique name and/or number for identifying and tracking user identity.

¹⁶ § 164.312.

¹⁷ § 164.312(a)(1).

Each covered entity must have the technical ability to assign unique identifiers for each user – person or machine. Entity identification may be necessary at the workstation, program or process, or record level, depending on the structure of the organization and its workforce.

WEDI SNIP suggests your risk analysis address the following questions:

- Does the organization have appropriate technical systems in place to allow for the assignment of unique user identifiers? Note that actual assignment and use of identifiers is addressed under administrative safeguards (see page 11). In addition, you need to ensure the systems can support and monitor the organization's requirements related to password management (see page 15).
- Can the technical systems be configured to grant access at various levels depending on the job function of each user? It may be necessary to control access at the program, process, or record level, depending on the data involved and the needs of each user?

Implementation Specification: Emergency Access Procedure (Required)

HIPAA Implementation Specification: Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

The need for access to ePHI may change during an emergency. Specifically, some job functions may be temporarily realigned necessitating different access to ePHI by workforce members. In addition, the need to restore and verify the integrity of the restored data may require different access by information technology personnel and others involved in disaster recovery.

WEDI SNIP suggests your risk analysis address the following questions:

- Does the contingency plan (see page 17) require different access to ePHI during an emergency?
- If so, do the technical systems have the ability to support such temporary changes in access? If not, the organization may have to implement new systems to support the contingency plan.
- Are there procedures for activating emergency access? The procedures should address who can authorize such access and under what conditions.

Implementation Specification: Automatic Log-off (Addressable)

HIPAA Implementation Specification: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

This is an addressable specification. Workforce members often walk away from workstations without logging off. This can be a security concern, particularly in areas with public access. Automatic log-off procedures can be implemented to minimize the likelihood that an unauthorized individual may access the workstation.

WEDI SNIP suggests your risk analysis address the following questions:

- Do the technical systems support automatic log-offs?
- Does the organization want to implement automatic log-offs? While addressable, it is likely that automatic log-offs will need to be implemented to reduce the risk of a security breach. Remember to monitor the use of log-offs and to minimize the ability of workforce members to override the automatic log-offs.

Implementation Specification: Encryption and Decryption (Addressable)

HIPAA Implementation Specification: Implement a mechanism to encrypt and decrypt electronic protected health information.

This implementation specification addresses the need to encrypt ePHI both at rest and transit. It is discussed further below under Standard: Transmission Security, page 30.

WEDI SNIP suggests your risk analysis address the following question:

- Has your organization evaluated the need to encrypt some or all of its data at rest? Consider, for example, the need to encrypt PHI on laptop computers and other mobile devices, for example.

Standard: Audit Controls¹⁸

HIPAA Implementation Specification: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

There are a wide variety of approaches to auditing systems. These range from tracking at the keystroke level (which may degrade system performance) to more generalized tracking, e.g., log-on tracking, which may not provide enough specific information to identify problems. It is important that system activity audits (1) are specific enough to identify security problems and (2) give the organization the ability to identify such potential problems which may be a time consuming task. There is great deal of discussion regarding what is the appropriate balance.

WEDI SNIP suggests your risk analysis address the following question:

- Are activity audit logs currently created? If so, are they sufficiently detailed to identify potential security problems and is the organization reviewing the logs in enough detail to identify such potential problems? If audit logs are not created or are not sufficient, the organization will have to change its current procedures.

Standard: Integrity¹⁹

HIPAA Standard: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

The focus of integrity is to ensure electronic confidential information is kept consistent with the source information and is not changed inappropriately. If a covered entity has implemented the policies and procedures discussed in this white paper, it has taken a series of reasonable steps aimed at ensuring the integrity of the data. This includes:

- Implementation Specification: Authorization and/or Supervision (Addressable) (page 9),
- Standard: Information Access Management (page 11),
- Implementation Specification: Protection from Malicious Software (Addressable) (page 14),
- Implementation Specification: Log-in Monitoring (Addressable) (page 14),

¹⁸ § 164.312(b).

¹⁹ § 164.312(c)(1).

- Implementation Specification: Password Management (Addressable) (page 15),
- Standard: Facility Access Controls (page 21),
- Standards: Workstation Use and Workstation Security (page 23),
- Standard: Device and Media Controls (page 24),
- Implementation Specification: Unique User Identification (Required) (page 26),
- Standard: Audit Controls (page 28),
- Standard: Person or Entity Authentication (page 29), and
- Standard: Transmission Security (page 30).

Implementation Specification: Mechanism to Authenticate Electronic Protected Health Information (Addressable)

HIPAA Implementation Specification: Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

It may be reasonable for your covered entity to implement specific electronic protocols to review ePHI and corroborate that it has not been inappropriately altered. This may involve doing electronic “spot checks” of the ePHI, comparing specific data fields, performing statistical analyses, and so forth. This can be a particularly complex undertaking.

WEDI SNIP suggests your risk analysis address the following questions:

- Has your organization evaluated the need to implement specific electronic procedures to corroborate the integrity of ePHI? If not, this should be accomplished.
- If your organization needs to implement specific electronic procedures, has your organization done such? If not, appropriate procedures must be identified and implemented.

Standard: Person or Entity Authentication²⁰

HIPAA Implementation Specification: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Covered entities must have in place appropriate technical processes to authenticate the identity of each person or entity (usually another computer or process) accessing or attempting to access PHI. This access can be at the workstation or program level, depending on the requirements of the organization. These technical processes usually require persons and entities to provide a password, a physical identification (e.g., a token) or biometric identification. Access of individuals is implemented through the administrative policies and procedures related to the use of passwords and individual access to ePHI. Similar policies and procedures must be in place to authenticate entities to ensure that ePHI is only shared with appropriate, authorized entities.

WEDI SNIP suggests your risk analysis address the following questions:

- Are appropriate measures in place to authenticate the identity of each person accessing or attempting to access PHI?
- Are appropriate measures in place to authenticate the identity of each entity accessing or attempting to access PHI?

²⁰ § 164.312(d).

Standard: Transmission Security²¹

HIPAA Standard: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Covered entities must implement mechanisms to ensure information is only transmitted to the intended individual or entity. Specifically, the standard includes two addressable implementation specifications: integrity controls and the use of encryption.

Implementation Specifications: Integrity Controls (Addressable) and Encryption (Addressable)

HIPAA Implementation Specification: Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

HIPAA Implementation Specification: Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Due to the increased use of messaging systems involving ePHI, care must be exercised before using e-mail or the Web to transmit ePHI. First, your organization should consider creating and implementing policies and procedures to address how and under what conditions ePHI can be transmitted. Unfortunately, most covered entities do not currently have such policies and procedures. Integrity controls must be put in place to protect ePHI transmissions and the use of electronic messaging must be secured. Securing transmissions requires some form of encryption.

In reality the risk of illicitly intercepting ePHI is generally low. However, the likelihood of incorrectly sending ePHI to the wrong individual is significant. Therefore, encryption should be utilized whenever applicable. Encryption can be utilized at the client (desktop), server (gateway) or at the Web portal. *It is important to note that an encrypted file cannot be scanned for viruses and spam.*

WEDI SNIP suggests your risk analysis address the following questions:

- Does the organization use or need to use electronic signatures? The electronic signature is currently the best way to verify that the data has not been altered. Most covered entities probably will not need to implement an electronic signature unless compliance is required with clinical trials involved under FDA 21 CFR Part 11 rule.
- Does the organization need to use encryption? If you are sending ePHI electronically via e-mail or over the Web, you should consider using encryption. Consider the following:
 - Interoperability: The ideal solution should work with various e-mail clients including older and less common products.
 - File Formats: The solution should accommodate standard e-mail messages along with various types of file attachments and file formats.
 - Scalability: The ideal solution should accommodate a large volume of e-mail traffic and attachments without consuming a large amount of processing resources.
 - Authentication: The solution should allow for the authentication of the sending and receiving entities. The solution should provide for effective and efficient key management.
 - Security: The solution should provide acceptable encryption strength and provide for the satisfactory protection of keys.

²¹ § 164.312(e)(1).

- Cost-effectiveness: The implementation of the solution should be cost-effective.
- Accuracy: Software should be considered that uses business rules and algorithms to search for ePHI to ensure it are encrypted.
- Virus checking and Content Filtering: The solution should allow for virus checking and content filtering of messages and their attachments.
- Ease of Use: The solution should be easy to use and implement by covered entities. The solution should be “transparent” to the end-user.

NIST/URAC/WEDI Initiative

The NIST/URAC/WEDI Health Care Security Workgroup was established in late 2002. In response to the HIPAA final Security Rule, the Workgroup was formed to facilitate the identification and implementation of best practices in health care for information security requirements and identify similarities between those practices and the HIPAA standards. The Workgroup held its first meeting in December 2002, and through a series of monthly, open forum meetings, is working to establish an ongoing dialogue to address issues relevant to security in health care systems and IT applications.

The *mission* of the Workgroup is to:

- facilitate communication and consensus on the best practices for information security in health care and
- promote the implementation of a uniform approach to security practices and assessments.

The *goals* of the Workgroup are to:

- identify security standards for future use in the health care industry and
- review and discuss security standards currently being used in the health care industry in order to drive consensus on best practice.

A Crosswalk Task Force has been established to provide a crosswalk of the HIPAA Security Rule requirements to existing security standards being used within the health care industry. The Task Force is planning to provide the health care industry with a crosswalk matrix to assist with effective implementation of HIPAA into existing health information security efforts by comparing various security standards, which may already be implemented, with the HIPAA security requirements.

The standards and processes being considered for review against the HIPAA Security Rule include:

- NIST Special Publication 800 Series
- ISO 17799
- CMS Core Security Requirements
- CMS Internet Security Requirements
- Federal Information System Control Manual (FISCAM)
- DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

The workgroup has developed a matrix to map the HIPAA Security Rule requirements to those of the other information security standards. This matrix is part of the NIST 800-66 DRAFT Publication (released June 2004). The goal is for entities to be able to review this matrix and more easily determine if they are meeting particular Security Rule standards. For example, if an entity is meeting the requirements of ISO 17799, and Security Rule requirements track to ISO 17799, then the entity can have some assurance that it already is

meeting the HIPAA requirement. In any case, it is recommended that entities use due diligence to ensure the HIPAA requirements are met.

If you have not specifically implemented any of the security standards included in the crosswalk, the matrix may still be useful in meeting the HIPAA requirements. Specifically, the HIPAA requirements are new and the security industry is just beginning to get familiar with those requirements. On the other hand, many in the security industry are familiar with the other standards to be included in the matrix, e.g., the NIST documents and ISO 17799. Informing security professionals that complying with a particular HIPAA requirement can be accomplished by meeting a familiar standard from another source will make it easier for them to help you implement the HIPAA requirements.

More information on the Workgroup can be found on the Security and Privacy Workgroup portion of the WEDI/SNIP Web site: snip.wedi.org.

Other Sources of Information

Resources specifically relevant to performing a risk assessment are as follows:

WEDI/SNIP Security and Privacy Whitepapers –

<http://snip.wedi.org/public/articles/index.cfm?Cat=48>.

NIST SP 800-26 – <http://csrc.nist.gov/publications/nistpubs/index.html>

NIST SP 800-66 - <http://cs-www.ncsl.nist.gov/publications/drafts/DRAFT-sp800-66.pdf>

Acknowledgments

WEDI/SNIP would like to express its appreciation to the authors for their efforts in preparing this White Paper:

Jon Bogen, President
HealthCIO Inc

Susan Brousseau, Senior Business Analyst
Medica Health Plans

Rick Ensenbach CISSP, CISA, CISM, Senior Security Consultant
Shavlik Technologies

Sub-Workgroup Leaders:

Lesley Berkeyheiser
The Clayton Group

Andrew Melczer, Ph.D., Vice President
Illinois State Medical Society

Appendix A: Security Standards Matrix

Administrative Safeguards

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	
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

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	
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

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	
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		Integrity Controls	(A)
		Encryption	(A)