



Managing Information Privacy & Security in Healthcare

The HIPAA Final Security Rule in Plain English

By Kristen Sostrom and Jeff Collmann Ph.D

This document includes a "Plain English" explanation for the general rules and each standard and associated implementation specifications in the Health Insurance Portability and Accountability Act of 1996, Security Standards, Final Rule. In this document, the standards and implementation specifications follow consecutively as found in the Final Rule. For each standard or implementation specification, the document provides the individual rule's identity (Standard or Implementation Specification), section number (e.g. §164.308(a)(1)(i)), title (e.g. Security Management Process), compliance status (Required or Addressable), and the text of the rule in **blue font**. Below this information, the document presents text explaining the rule in "Plain English". The "Plain English" text often appears longer than the text of the rule because it explains the meaning and offers guidance for action.

[§164.306 Security Standard: General Rules](#)

The General Rules section of the HIPAA Security Rule provides the objective and scope for the data security rule as a whole. The unique and often sensitive nature of individually identifiable health information means that misuse can damage, threaten or embarrass the individual it concerns. A covered entity must, therefore, develop a program that includes a range of safeguards to protect it. HIPAA defines protected health information (PHI) as the subset of individually identifiable health information that is maintained or transmitted in any form or medium except for information in records covered by the Family Educational Rights and Privacy Act and employment records held by a covered entity in its role as employer. The HIPAA Privacy Rule covers PHI in all forms (paper, oral and electronic). The HIPAA Security Rule applies only to protected health information that is maintained or transmitted in electronic form (E PHI). The HIPAA data security rule for the most part does not prescribe specific safeguards for all covered entities to use regardless of their circumstances. Rather, it expects each covered entity to evaluate its protection approach in light of its mission, budget and good information assurance practices. This section includes five detailed explanations, including General requirements, Flexibility of Approach, Standards, Implementation Specifications and Maintenance

§164.306(a) General requirements. Covered entities must do the following:

(1) Ensure the confidentiality, integrity and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and (4) Ensure compliance with this subpart by its workforce.

Section (a) General requirements establishes four general objectives, including: 1) Covered entities must institute controls on electronic protected health information they collect, use, maintain, store and transmit that restrict access to only authorized individuals, ensure its accuracy and completeness, and provide access to authorized individuals when required. 2) Covered entities must protect that information from reasonably anticipated threats or hazards. A threat is an event that can result in the unauthorized disclosure, modification, destruction or interruption to the information. While threats can come in many forms and from many sources, this standard applies the rule of reasonableness. A covered entity does not need to protect health information from threats they cannot anticipate or have some reason to expect will not occur. For example a medical facility located in Kansas does not need to develop safeguards against the threat of a hurricane but should ensure they are protected in the event of a tornado. 3) Covered entities must ensure that the information is used and disclosed only as permitted by the HIPAA Privacy Rule (subpart E). The HIPAA Security Rule and Privacy Rule should work together. The Privacy Rule defines how the information should be used, providing rules for disclosure and access. The Security Rule defines the safeguards an entity must use to implement and enforce the standards defined in the Privacy Rule. 4) Finally covered entities must ensure that the people they employ implement and abide by all of the standards and implementation specifications put forth in the HIPAA Security Rule. Covered entities must meet these objectives through the development, implementation, maintenance, and documentation of administrative, physical, and technical safeguards.

§164.306(b) Flexibility of Approach

(1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementations as specified in this subpart.

(2) In deciding which security measures to use, a covered entity must take into account the following factors:

- i. The size, complexity, and capabilities of the covered entity.
- ii. The technical capabilities of record systems used to maintain electronic protected health information.
- iii. The costs of security measures.
- iv. The probability and criticality of potential risks to electronic protected health information.

The rule adopts a flexible approach to compliance allowing covered entities to adopt protection measures as appropriate. Protection strategies and tactics may vary depending on a covered entity's size, complexity and capabilities, the hardware and software security capabilities of its technical infrastructure, the cost of

security measures and the probability and criticality of potential risks. This language implicitly emphasizes the continued important role of organizational and technical risk assessments in establishing the conditions for compliance with the HIPAA data security rules.

[§164.306\(c\) Standards](#). A covered entity must comply with the standards described in [§164.308](#), [§164.310](#), [§164.312](#), [§164.314](#), and [§164.316](#) with respect to all electronic protected health information

This section requires covered entities to comply with the standards and implementation specifications found in the subparts of the HIPAA Security Rule titled administrative safeguards, physical safeguards, technical safeguards, organizational requirements, and policies and procedures and documentation requirements. These standards and implementation specifications provide a more detailed picture of how a covered entity should meet the objectives stated in the general rules.

[§164.306\(d\) Implementation Specifications](#)

In this subpart:

(1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.

(2) When a standard discussed in §164.308, §164.310, §164.312, §164.314, and §164.316 includes required implementation specifications, a covered entity must implement them.

(3) When a standard discussed in §164.308, §164.310, §164.312, §164.314, and §164.316 includes implementation specifications that must be addressed, a covered entity must—

i. Assess whether each such implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and

ii. As applicable,

A. Implement the implementation specification when reasonable and appropriate; or

B. If implementing the implementation specification is not reasonable,

(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

This section explains the difference between "required" and "addressable" implementation specifications. Covered entities must implement all implementation specifications labeled as "required". Covered entities must evaluate implementation specifications with an "addressable" label as part of their information security

risk assessment and determine their applicability. If the risk analysis determines that the implementation specification is reasonable and appropriate for the environment, the covered entity must implement the safeguard. If the safeguards to implement the implementation specification are not reasonable or appropriate, the covered entity must document the rationale for not implementing the specification. If other safeguards can be used to meet the standard that make more sense for the covered entity's environment and way of doing business, the covered entity must document its use of those alternative safeguards.

[§164.306\(e\) Maintenance.](#)

[Security measures implemented to comply with standards and implementation specifications adopted under §164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at §164.316](#)

This section requires maintenance of the organization's security measures consistent with the organizational and documentation requirements and of HIPAA. Neither the way a covered entity does business, nor the threats to protected information remain static. As new technology emerges and business processes change, the covered entity must review and update the security measures used to implement these standards. §164.316 entitled, "Policies and Procedures and documentation requirements", requires covered entities to document in electronic or other written form all policies and procedures as well as specified actions, activities or assessments implemented to comply with the HIPAA data security rules. A covered entity must retain such documentation for six years from the date of its creation or the date when it was last effective, whichever is later. It must make the documentation available to persons responsible for implementing relevant procedures. It must also periodically review and update documentation as changes affect the security of a covered entity's EPHI.

[1.0 Standard §164.308\(a\)\(1\)\(i\) Security Management Process \(Required\)](#)

[Text: "Implement policies and procedures to prevent, detect, contain, and correct security violations."](#)

The security management process and its related implementation specifications form the foundation of a covered entity's entire security program. This standard mandates a "life cycle approach" to security; that is to say, an organization must assess its security posture and work to reduce its risks on a continual basis as the security environment and needs of the organization change. To meet this requirement all levels of a covered entity's management must participate in the compliance process. To emphasize the importance of this requirement all four of the security management process implementation specifications are required, namely risk analysis, risk management, sanction policy, and information system activity review.

[1.1 Implementation Specification §164.308\(a\)\(1\)\(ii\)\(A\) Risk Analysis \(Required\)](#)

[Text: "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."](#)

Each covered entity must conduct a risk analysis. A risk analysis or risk assessment includes a threat assessment, vulnerability pairing, and residual risk determination. The risk analysis should include organizational and technical assessments that address all areas of security, not only the information

systems. When selecting protection measures, covered entities should balance costs with projected losses as a criterion. Because HIPAA compliance depends upon risk assessment, covered entities may legitimately select different solutions to similar problems depending upon individual circumstances. No single approach to HIPAA compliance exists or meets the needs of all covered entities.

1.2 Implementation Specification §164.308(a)(1)(ii)(B) Risk Management (Required)

Text: "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306 (a)."

Each covered entity must implement security measures, including policies, procedures, and technical controls to comply with the HIPAA Security and Privacy Rules. This requirement highlights the cyclical nature of information security management. Building on the first mandatory implementation specification, risk analysis, the risk management process requires a covered entity to develop plans and take actions in response to the risk analysis as well as sponsor subsequent reassessments to determine the effectiveness of implemented safeguards. The reference to §164.306(a) puts the risk management efforts into context. The objectives of risk management must include protecting electronic PHI against violations of the use and disclosure requirements found in the HIPAA Privacy Rule and ensuring compliance with the HIPAA Security Rule. A risk based security management process uses the results of periodic risk analyses continually to maintain and improve the organization's security posture.

1.3 Implementation Specification §164.308(a)(1)(ii)(C) Sanction Policy (Required)

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

Each covered entity must implement policies and procedures for disciplining employees for breaches of the security of EPHI. Those violations include failure to comply with the organization's policies and procedures. An investigation following the covered entity's standard disciplinary process will determine the specific sanction according to the severity and circumstances of the violation.

1.4 Implementation Specification §164.308(a)(1)(ii)(D) Information System Activity Review (Required)

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

Each covered entity must review their records of system activity. As we all know it does no good to produce records of system use such as audit and system logs if no one ever examines them for potential breaches of security policy. HIPAA does not distinguish between automated or manual logs and reports in this requirement. Both must be reviewed. HIPAA relies on a covered entity's risk analysis and risk management process to determine the frequency of audit review.

2.0 Standard §164.308(a)(2) Assigned Security Responsibility (Required)

Text: "Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity."

Each covered entity must assign formal responsibility for HIPAA security to one individual. The number and type of people required to implement an organization's security policies in a manner consistent with HIPAA will depend on the size and structure of the organization. The larger and more complex the organization, the greater the number of people needed. The actual number and the breakdown of responsibility should be determined as part of the security management process, particularly the risk assessment. Covered entities should document the identities and tasks of the officials responsible for health information security. No implementation specifications appear under assigned security responsibility.

3.0 Standard §164.308(a)(3)(i) Workforce Security (Required)

Text: "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."

The term "all members of its workforce" in this instance requires a very broad interpretation that includes all personnel with access to patient information whether or not they are directly involved in patient care. It includes a covered entity's own full-time and part-time employees, contract personnel, volunteers, students and trainees. Emphasis is placed on including those who do not normally access EPHI such as cleaning personnel or the occasional maintenance or repair contractor. Three addressable implementation specifications relate to workforce security, namely authorization and/or supervision, workforce clearance procedures, and termination procedures. Each of these requirements must be assessed in light of the risk assessment and implemented as part of the workforce security program if appropriate.

3.1 Implementation Specification §164.308(a)(3)(ii)(A) Authorization and/or Supervision (Addressable)

Text: "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."

Because this specification is "addressable", compliance depends on the outcome of a covered entity's risk assessment. If the risk assessment determines that threats exist from members of the workforce working with or in locations accessible to EPHI, a covered entity should institute procedures to ensure workforce members working in those locations are either authorized to be there, supervised while there or both. The choice may vary across different types of workers depending on the results of the risk analysis, cost and a covered entity's resources and business processes. The text broadens the criteria to include those with physical access to the network that do not necessarily have authorization or a "need to know" for information on the network. If the risk assessment determines that little threat exists, the covered entity may choose to take little action. The risk management plan should document the results and justify all actions taken in response to the risk assessment.

3.2 Implementation Specification §164.308(a)(3)(ii)(B) Workforce Clearance Procedures (Addressable)

Text: "Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate."

Because this requirement is “addressable”, compliance depends on the outcome of a covered entity’s risk assessment. Do not confuse clearance and authorization. “Clearance” is the process of determining a person’s trustworthiness. “Authorization” is the process of giving user permission to access information. A person can be “cleared” but still not authorized for access to certain information and vice versa. For example, policy may require that all personnel responsible for conducting and recording patients’ diagnostic tests have a National Agency Check (NAC) when hired. Technicians working in radiology and the lab would both have the same “clearance” but the radiology technician may not have “authorization” for access to the lab software and vice versa. This specification does not require that all personnel have a government/military style clearance. Rather, based on the results of its risk assessment, an organization should determine what type of screening process to use for each job position or role and document the procedures to be followed in conducting that check. Some roles may not require any process beyond an interview. Others may require job references and, still others, a NAC.

3.3 Implementation Specification §164.308(a)(3)(ii)(C) Termination Procedures (Addressable)

Text: “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.”

Because this requirement is “addressable”, compliance depends on the outcome of a covered entity’s risk assessment. This implementation specification focuses on two common threats: 1) the threat of continued access to information of terminated employees, and 2) continued access to information by those who are still employees but whose access is no longer appropriate. Employment can end for a variety of reasons such as retirement, change of jobs, or unsatisfactory performance with each reason potentially posing different threats to information assets. A covered entity may require various, differing procedures for terminating a former employee’s information access depending on the risk represented. The appropriateness of an employee’s access can change both permanently or temporarily during the course of their employment. A procedure should exist that terminates access when required by the clearance process. A covered entity should document its procedures for terminating access to information in its risk management plan.

4.0 Standard §164.308(a)(4)(i) Information Access Management (Required)

Text: “Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

This standard and the following related implementation specifications concern the administrative aspects of access controls, specifically the policies and procedures governing who may access what types of health information. While not specifically calling for access control based on roles, this rule does require differentiating information access given to different categories of worker. The degree of access differentiation depends on the results of the organization’s risk analysis, size, structure, and business needs based on the minimum necessary requirements found in the HIPAA Privacy Rule (subpart E). When looked at as a complete process, a typical hospital would have the following components to information access management. A hospital would first establish a set of policies that lists and describes the various categories of worker, the types of information needed by each category of worker, and permitted uses (read, write, amend) of each type of information for each category of worker. Access policies must also

reasonably limit information used on a routine or recurring basis to the minimum amount needed to achieve the purpose of the use. These rules should also include a process for handling exceptions to the stated access rules. This standard does not require technical controls to limit access to the minimum amount of information needed to perform their job functions. A second set of policies and procedures should describe authorization of accounts: how each category of worker is granted access to information and who has the authority to validate each step in the process including assigning workers to categories. A corresponding set of policies and procedures in the IT department should describe the process for setting up new accounts including what applications, permissions and resources should be granted to a new account based on the category assigned to the individual. And finally a set of policies and procedures should describe how to make changes to established accounts. A complete set of policies should include requiring a periodic review of accounts to validate that permissions and rights are current and accurate. These components can be grouped in to the two addressable implementation specifications, Access Authorization, and Access Establishment and Modification, which emphasize the types of processes that may need to be included in information access management based on the risk assessment and the business needs of the organization.

4.1 Implementation Specification §164.308(a)(4)(ii)(A) Isolating health care clearinghouse functions (Required)

Text: "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.

Each clearinghouse that is part of a larger organization must isolate their functions from those of the larger organization. A clearinghouse may be part of a larger organization that has functions unrelated to that of the clearinghouse (receiving, reformatting, and transferring health data). This specification requires that such clearinghouses must implement policies and procedures that protect the EPHI in the clearinghouse from those who work outside of the clearinghouse and are not authorized to access it.

4.2 Implementation Specification §164.308(a)(4)(ii)(B) Access Authorization (Addressable)

Text: "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."

Because this requirement is addressable, compliance depends on the outcome of a covered entity's information security risk assessment. As part of their information security risk assessment, covered entities should evaluate the need for policies and procedures governing how a potential user obtains the right to use specific information resources. Covered entities should prepare and document in their risk management plan appropriate policies and procedures for granting individuals access to information assets. These should include what authorizations and clearances are needed before an account can be established.

4.3 Implementation Specification §164.308(a)(4)(ii)(C) Access Establishment and Modification (Addressable)

Text: "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.

Because this requirement is addressable, compliance depends on the outcome of a covered entity's information security risk assessment. Once individuals receive appropriate authorization for access to information assets, the IT department must correctly enroll them into the system. During a risk assessment, a covered entity should address the need for procedures for establishing accounts in, or connections to the information system for each person, role and/or system, and documentation and regular review of those accounts. The risk management plan should explain and justify the covered entity's approach to system enrollment. No organization remains static. As people change jobs within an organization or business processes change, a covered entity will need to change access rights for individuals, roles and/or systems. For example when a physician becomes an administrator and stops seeing patients, he or she may no longer need routine access to patient files but may need access to quality assurance data to execute the new job. When an organization restructures its business or adds new services, it should review job descriptions and system performance in order to revise rules for controlling access to information assets. As part of their information security risk assessment, covered entities should evaluate the need for policies and procedures governing modification of access rights for individuals and/or systems. Covered entities should prepare and document in their risk management plan appropriate policies and procedures for modifying individual and system access to information assets if warranted. In conjunction with sound access termination rules (section 164.308(a)(3)(ii)(C)) and regular review of access authorizations, access modification rules ensure that the access granted to a person or system remains appropriate.

5.0 Standard §164.308(a)(5)(i) Security Awareness and Training (Required)

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

The writers of HIPAA considered security awareness and security training to be separate activities. Security "awareness" emerges through continuous activity to heighten staff consciousness of security, such as posters, periodic email reminders, and wording in headers and footers. "Training" functions as a discrete activity designed to teach someone security practices. The standard requires that all members of an organization's workforce participate in the program. There are four addressable implementation specifications associated with this standard.

5.1 Implementation Specification §164.308(a)(5)(ii)(A) Security Reminders (Addressable)

Text: "Implement periodic security updates."

Because this implementation specification is addressable, compliance depends on the outcome of a covered entity's information security risk assessment. Security reminders are an effective means to increase security awareness and strengthen an entity's security posture. Over time people tend to become comfortable in their surroundings and everyday security practices become lax. Covered entities should deploy security reminders in the form of e-mail messages, newsletters, posters and other means as part of the risk management process. As part of their information security risk assessment, covered entities should evaluate the need for policies and procedures to make staff, volunteers, contractors and all other users of protected health information aware of security concerns on a periodic ongoing basis. Covered entities

should prepare and document in their risk management plan, appropriate procedures for alerting users to issues in protecting the confidentiality, integrity and availability of protected health information. Covered entities should also maintain records documenting implementation of their security awareness plan.

5.2 Implementation Specification §164.308(a)(5)(ii)(B) Protection from Malicious Software (Addressable)

Text: "Implement procedures for guarding against, detecting, and reporting malicious software."

Because this implementation specification is addressable, compliance depends on the outcome of a covered entity's information security risk assessment. Viruses and other forms of malicious mobile code pose a significant threat to most organizations that use information technology today. Automated virus detection programs protect against this threat. As part of their information security risk assessment, covered entities should evaluate the need for policies and procedures to inform staff, volunteers, contractors and all other users of protected health information of the threat of malicious software. Covered entities should prepare and document in their risk management plan, appropriate procedures for alerting users to potential harm of malicious software, methods of virus prevention, and response to virus detection. Covered entities should also maintain records documenting implementation of their malicious software education plan.

5.3 Implementation Specification §164.308(a)(5)(ii)(C) Log-in Monitoring (Addressable)

Text: "Implement procedures for monitoring log-in attempts and reporting discrepancies."

Because this implementation specification is addressable, compliance depends on the outcome of a covered entity's information security risk assessment. The log-in screen on many operating systems displays information concerning past log-in attempts including the user name last used during log-in, the date and time of the last successful log-in and the number of unsuccessful log-in attempts since the last successful log-in. This information can alert users to possible unauthorized access attempts from that workstation. As part of their information security risk assessment, covered entities should assess the value of training personnel to monitor and report log-in discrepancies, based on the capabilities of their systems and other safeguards in place. If the risk management process indicates this safeguard is appropriate, covered entities should include policies and procedures describing this training in their risk management plan.

5.4 Implementation Specification §164.308(a)(5)(ii)(D) Password Management (Addressable)

Text: "Implement procedures for creating, changing, and safeguarding passwords."

Because this implementation specification is addressable, compliance depends on the outcome of a covered entity's information security risk assessment. As part of their information security risk assessment, covered entities should assess the value of training personnel in the organization's password policies and how to create, change, and protect passwords. If the risk management process indicates this safeguard is appropriate, covered entities should include policies and procedures describing password training in their risk management plan.

6.0 Standard §164.308(a)(6)(i) Security Incident Procedures (Required)

Text: "Implement policies and procedures to address security incidents."

This standard requires a covered entity to develop a plan for handling security incidents and breaches. The resulting policies and procedures should cover all potential categories of incidents. Examples include policy violations by users, denial of service attacks, intrusions, and unauthorized disclosures. This standard includes one related mandatory implementation specifications, "Response and Reporting Procedures".

6.1 Implementation Specification §164.308(a)(6)(ii) Response and Reporting Procedures (Required)

Text: "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."

Each covered entity must document in advance procedures for how it will identify, respond to and document an incident. Response procedures need to be developed for both major and minor incidents. Entities can obtain guidance from many emergency response organizations on how to respond to major incidents. Covered entities have a responsibility to mitigate any known harmful effects of a security incident or breach to the extent that is practicable. It is important to keep in mind when developing response procedures that determining the extent and potential magnitude of an incident may be difficult when first discovered. Yet, an incident may have many critical short and long-term effects on an organization. Thus, an organization's initial response to an incident may have a dramatic impact either mitigating or exacerbating short and long-term impacts. A covered entity's policies must include procedures for documenting any incidents or breaches that occur, how it responds and the results and/or impact on its operations. The covered entity must retain the documentation for a period of six years as required by § 164.316 (b)(1)(ii).

7.0 Standard §164.308(a)(7)(i) Contingency Plan (Required)

Text: "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.

In the modern world, organizations that deploy computerized patient record systems should assume that disasters happen. Thus, preparing a contingency plan constitutes a fundamental element in a covered entity's information security risk management plan. This standard requires a covered entity to create and periodically update a contingency plan. Three required and two addressable implementation specifications explain and expand on elements of a contingency plan.

7.1 Implementation Specification §164.308(a)(7)(ii)(A) Data Backup Plan (Required)

Text: "Establish policies and procedures to create and maintain retrievable exact copies of electronic protected health information."

Each covered entity must create and maintain data backups. The "data backup" portion of a contingency plan should ensure that information will not be lost in the event of a major system loss. The rule requires a covered entity's health information system contingency plan to include procedures for performing "exact

copies” of individually identifiable patient information (backups) for retrieval when necessary. A covered entity should determine what information requires back up, the appropriate backup mechanism (e.g., magnetic tapes, paper, or other medium), how to maintain the backups (e.g., offsite, in an air conditioned compartment or other conditions), and duration of maintenance (e.g., six months or following state or other guidelines for patient records) as part of its risk analysis including its application and data criticality analyses. The covered entity’s contingency plan should document the backup policies and procedures, including provisions for periodically reviewing and updating them.

7.2 Implementation Specification §164.308(a)(7)(ii)(B) Disaster Recovery Plan (Required)

Text: “Establish (and implement as needed) policies and procedures to restore any loss of data.”

Each covered entity must have a plan for recovering from a disaster. Fire, vandalism, natural disaster, system failure and other unusual events occasionally damage protected health information and pose great risks to patient care and healthcare operations. This required implementation specification requires covered entities to include in their information system contingency plans a strategy and method for recovering lost or inaccessible protected health information in a timely manner after a disaster. Their risk analyses including application and data criticality analysis will determine the order, interval of time, and the methods chosen for recovery.

7.3 Implementation Specification §164.308(a)(7)(ii)(C) Emergency Mode Operation Plan (Required)

Text: “Establish (and implement as necessary) policies and procedures to enable continuation of critical business processes for the protection of the security of electronic protected health information while operating in emergency mode.”

Each covered entity must plan to protect PHI during an emergency. Fire, vandalism, natural disaster, or system failure sometimes damage safeguards to the confidentiality, integrity and availability of protected health information. This implementation specification requires covered entities to develop and implement alternate means of protecting health information during such emergencies until normal controls are restored. Covered entities will identify appropriate approaches to this problem during their information security risk assessment and document them in their contingency plans.

7.4 Implementation Specification §164.308(a)(7)(ii)(D) Testing and Revision Procedures (Addressable)

Text: “Procedures for periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.”

Because this implementation specification is “addressable”, compliance depends on the outcome of a covered entity’s risk assessment. Testing serves two well-known purposes; namely training for those who must carryout a contingency plan and assurance that the plan is appropriate and will work. Failures in the testing process provide a means for correcting and improving the plan thus providing something that will work in the event of a real emergency. Testing of successful plans needs to occur on a periodic basis to refresh the training and to ensure that the plans remain appropriate as business processes and the environment change over time. If sites do not incorporate testing and revision procedures into the contingency plan, they must explain their reasons in their risk management plans.

7.5 Implementation Specification §164.308(a)(7)(ii)(E) Applications and Data Criticality Analysis (Addressable)

Text: "Assess the relative criticality of specific applications and data in support of other contingency plan components."

Because this implementation specification is "addressable", compliance depends on the outcome of a covered entity's risk assessment. A comprehensive information security risk assessment should include analyses of the relative importance, exposure to threat, and existing safeguards of a site's various health information assets, including applications and data. The results of the application and data criticality analysis help assign priority to information assets and determine appropriate protection strategies. This rule emphasizes that the results of the criticality analyses should affect preparation of a contingency plan. The risk assessment should drive an applications and data criticality analysis. The site should use information from that analysis in preparing its contingency plan.

8.0 Standard §164.308(a)(8) Evaluation (Required)

Text: "Perform a periodic technical and non-technical evaluation that 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 subpart."

This evaluation should examine the entire security posture of the organization beginning with requirements of the HIPAA Security Standard Final Rule and, subsequently, as part of an organization's response to changing conditions from outside and inside its own boundaries. "Environmental" conditions include changing security-related international, national, state, or local mandates that apply to the business being certified as well as novel threats. "Operational" changes include the implications of changes in mission, business practices and technology. Identifying relevant requirements should occur as part of the ongoing process of information security risk management. Linking the Evaluation effort to risk management emphasizes the "life-cycle" approach to risk management outlined as part of the security management process and thereby brings risk management full circle. Good risk management plans become incorporated into everyday practice and do not disappear into an administrative drawer once signed. By documenting that they are providing the level of protection promised at the beginning of the process, covered entities demonstrate their compliance with this fundamental strategic goal of health information assurance. Evaluations of equipment by standards organizations do not suffice, as the technical security features of the computer system hardware and software constitute only one aspect of an organization's security program.

9.0 Standard §164.308(b)(1) Business Associate Contracts and Other Arrangements (Required)

Text: "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, in accordance with §164.314(a) that the business associate will appropriately safeguard the information.

(2) This standard does not apply with respect to--

(i) The transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual

(ii) The transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of §164.314(b) and § 164.502(f) apply and are met; or

(iii) The transmission of electronic protected health information from or to other agencies providing the services at § 164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)(C) are met.

(3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and §164.314(a)."

The security notice of proposed rulemaking (NPRM) specified "chain of trust" agreements when a covered entity processed data through a third party, including organizations which otherwise qualified as "covered entities" as well as non-covered entities. The final rule restricts the requirement to exchanges of information with non-covered entities and harmonizes the process with the requirements of the HIPAA privacy final rule for business associates. Covered entities can draft the written agreements in the form of a contract or other legal document and may deal with security as the sole topic or as part of a broader contract or document between the two parties. When the covered entity and the business associate are both governmental entities, they may use a memorandum of understanding (MOU) in place of a contract.

The contracts or memoranda must require the business associate to implement administrative, physical and technical safeguards providing a minimum level of protection equivalent to that required by the final rule for security and the use and disclosure rules of the Privacy Rule. The business associate must agree to ensure that any agents or subcontractors to whom it provides information will also implement equivalent safeguards, report any security incidents to the covered entity and make its policies, procedures and related documentation available to the Department of Health and Human Services for determining compliance as needed. The contracts or legal document must allow the covered entity to terminate the contract if the business associate violates the terms of the contract on data security. Governmental agencies may omit the termination clause from the MOU if it is contrary to the legal obligations of the business associate or covered entity. This ensures that health information that is protected by a provider, health plan or clearinghouse continues to be protected when given to someone that is not required to comply with HIPAA.

Three exemptions exist to this standard, including:

1. When providing protected health information in connection with treatment of a patient, a covered entity need not enter into a business associate contract with health care providers.
2. Contracts are not required between a group health plan and the plan sponsor. The group health plan must document that the plan sponsor will protect any electronic PHI other than summary information created, received, used or disclosed in association with the health plan.

3. Government programs that provide public benefits need not enter contracts or MOUs with other agencies providing enrollment and eligibility determination services as authorized by law. Covered entities should refer to § 164.502 of the Privacy Rule for details of requirements affecting the uses and disclosures of protected health information. One required implementation specification exists with this standard.

9.1 Implementation Specification §164.308(b)(4) Written Contract or Other Arrangement (Required)

Text: “Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).”

Each covered entity must have written contracts and arrangements that meet HIPAA requirements. This mandatory implementation specification emphasizes that the business associate contracts, MOUs or other legal agreements must be in writing. The content of those agreements as required in the standard above must be explicitly documented.

10.0 Standard §164.310(a)(1) Facility Access Controls (Required)

Text: “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.”

Physical access controls should permit entry to individuals with appropriate authorization and deny entry to individuals lacking appropriate authorization. This standard requires limiting physical access both to the general building or business suite and to areas dedicated to the storage and use of computer equipment and media. Four addressable implementation specifications supplement this mandatory requirement, including contingency operations, facility security plan, access control and validation procedures, and maintenance records. These physical controls reinforce both the administrative and technical policies and procedures on information access management required elsewhere in the rule. The administrative, physical, and technical controls collectively protect the confidentiality, integrity and availability of protected health information by permitting only authorized individuals to create, review or modify only information for which they have a “need-to-know”.

10.1 Implementation Specification §164.310(a)(2)(i) Contingency Operations (Addressable)

Text: “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.”

Because this implementation specification is addressable, compliance depends on the outcome of a covered entity’s information security risk assessment. Some overlap exists between Contingency Operations under “Facility Access Controls” and Contingency Planning under “Administrative Procedures”. This rule focuses attention on the functioning of the facility and its access control mechanisms (both administrative and technical) during and after an emergency or disaster. A covered entity must include evaluating threats to the correct functioning of physical access controls during an emergency and during efforts to recover from disasters as part of its information security risk assessment. A covered entity must

document its plans for assuring appropriate physical access during emergencies and disaster recovery efforts in its risk management plan.

10.2 Implementation Specification §164.310(a)(2)(ii) Facility Security Plan (Addressable)

Text: "Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft."

Because this implementation specification is addressable, compliance depends on the outcome of a covered entity's information security risk assessment. A covered entity must evaluate the need for, and adequacy of controls on physical access to facilities and equipment handling protected health information as part of its information security risk assessment. As part of its risk management plan, a covered entity should document its approach to controlling physical access to facilities and equipment handling protected health information. A good facility security plan will include policies, procedures and practices that always and only provide authorized, necessary access to health information assets during routine and emergency operations. If a covered entity does not control the building they occupy or shares space with other organizations, it nonetheless remains responsible for considering facility security. It can incorporate security measures into contracts with the party responsible for the building and document them in their own facility security plan.

10.3 Implementation Specification §164.310(a)(2)(iii) Access Control and Validation Procedures (Addressable)

Text: "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."

Because this implementation specification is addressable, compliance depends on the outcome of a covered entity's information security risk assessment. As part of its information security risk assessment, a covered entity must evaluate the need for procedures that provide individuals' physical access only to the "minimum necessary" data they "need-to-know" in order to discharge their job responsibilities. As part of their information security risk assessment, covered entities must evaluate the need for policies and procedures for the following access controls;

1. Validating identity and access authorizations of people requesting access to a building, suite, controlled rooms and/or computer equipment prior to allowing access;
2. Controlling the flow of visitors through its facilities including patients, vendors and guests;
3. Permitting only authorized personnel to enter a site where software programs that manage EPHI are tested and revised.

Their risk management plan must justify their decision and explain any physical access controls adopted on the basis of that principle. This rule complements the access control requirement found in the category, "Administrative Procedures". Under the "Administrative Procedures" category, covered entities must implement controls that establish different levels of access to information depending on work needs. From the perspective of the user, controlling physical access to areas within the facility with "need-to-know"

procedures supports and strengthens the protective function of differentiating levels of general access to information stored and processed within the facility.

10.4 Implementation Specification §164.310(a)(2)(iv) Maintenance Records (Addressable)

Text: "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, or locks)."

Because this implementation specification is addressable, compliance depends on the outcome of a covered entity's information security risk assessment. As part of their information security risk assessment, covered entities must evaluate the need for keeping a record of the repairs and modifications to the physical components of a facility containing EPHI. The risk management plan should document the results and justify all actions taken in response to the risk assessment. Such procedures ensure accountability and aid in maintaining the facility security plan and other safeguards.

11.0 Standard §164.310(b) Workstation Use (Required)

Text: "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 a class of work station that can access electronic protected health information."

Workstation" includes any electronic device used to input and/or process health information such as laptops, personal computers or computer terminals. This standard applies only to workstations that can be used to access protected health information and requires documentation of the functions and performance of those workstations. Covered entities should evaluate threats and vulnerabilities to workstations and to protected health information accessible through the workstation during the risk assessment process. The risk management plan must justify and describe controls instituted to mitigate threats to workstations and associated PHI, including specification of the appropriate physical environment for the workstation. This can be accomplished by addressing the needs of individual workstation or types of workstations. There are no associated implementation specifications with this standard.

12.0 Standard §164.310(c) Workstation Security (Required)

Text: "Implement physical safeguards for all workstations that access electronic protected health, to restrict access to authorized users."

This standard complements standard §164.310(b) by requiring covered entities to implement physical controls that grant workstation access to authorized users and prevent workstation access to unauthorized users. In its information security risk assessment, a covered entity must evaluate the threats and vulnerabilities of inappropriate physical access to workstations by unauthorized personnel. In its risk management plan, it must describe and justify the controls instituted to mitigate such threats and vulnerabilities. There are no associated implementation specifications with this standard.

13.0 Standard §164.310(d)(1) Device and Media Controls (Required)

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

The standard requires covered entities to develop policies and procedures that will guard the EPHI on hardware and movable media. Media includes drives, diskettes, compact discs, tapes and any other device that is capable of storing electronic information. The movement of these devices must be protected within a facility and when they enter or leave a facility. Four associated implementation specifications expand on aspects of media controls, including: disposal, media reuse, accountability, and data backup and storage.

13.1 Implementation Specification §164.310(d)(2)(i) Disposal (Required)

Text: "Policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which electronic protected health information is stored."

Each covered entity must implement safeguards for the disposal of EPHI, hardware and electronic media. As covered entities replace and update hardware and other media, EPHI can remain on hard drives and other media. This implementation specification requires policies and procedures for preventing EPHI from being disclosed while disposing of EPHI or electronic media and devices used to store EPHI. Policies and procedures should include approved methods of disposal such as use of commercial or public disposal services, sale or donation of electronic devices and the process for ensuring that EPHI processed by or stored on the hardware and electronic media is no longer accessible.

13.2 Implementation Specification §164.310(d)(2)(ii) Media Re-use (Required)

Text: "Procedures for removal of electronic protected health information from electronic media before the media is made available for re-use, (for example, by reformatting, writing over existing data, and use of special demagnetizing (degaussing) equipment)."

Each covered entity must remove EPHI before electronic media is re-used. Electronic devices and media are often reused in the normal course of business. For example new employees often receive workstations used by previous employees. This implementation specification requires that the covered entity establish procedures for authorizing media for re-use and for removing PHI before re-use depending on the environment and the sensitivity of the information. Although some overlap exists with §164.310 (d)(2)(iv) Disposal, this implementation specification emphasizes all possible re-uses of the media or electronic devices by personnel and systems inside and outside of the covered entity. Disposal concerns discarding of the media, which might include reuse by persons or systems outside the organization. A covered entity's risk management plan should describe and justify procedures for implementing the media re-use policies.

13.3 Implementation Specification §164.310(d)(2)(iii) Accountability (Addressable)

Text: "Maintain a record of the movements of hardware and electronic media and any person responsible therefore."

Because this requirement is "addressable", compliance depends on the outcome of a covered entity's risk assessment. Staff of covered entities often process and store protected health information on highly

portable, electronic media thus creating a potential for theft or loss. A covered entity's policies must require evaluating the need for procedures to mitigate this threat as part of its information security risk assessment. A covered entity should describe and justify as part of its risk management plan procedures for safely managing electronic devices and media, including records of who, when, and where possesses devices or media from the time of original receipt to time of final disposal or transfer to another entity. The mechanism used for recording this information may be manual or automated.

13.4 Implementation Specification §164.310(d)(2)(iv) Data Backup and Storage (Addressable)

Text: "Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."

Because this implementation specification is "addressable", compliance depends on the outcome of a covered entity's risk assessment. Covered entities must perform data backup as part of the contingency plan requirement (see §164.308(a)(7)(ii)(A) Data Backup Plan). As part of the device and media control requirement in physical safeguards, this addressable implementation specification stipulates controls governing the movement and availability of backups. Electronically stored information can be lost, damaged, or destroyed if stored improperly or when equipment is moved. A covered entity should address threats to the confidentiality, integrity and availability of protected health information on equipment being moved and during storage in its information security risk assessment. The risk management plan should describe and justify its approach to issues such as secure movement of equipment, media shelf life and retention periods, the conditions of short and long-term storage locations, and physical protection measures for media repositories. Covered entities should document policies as part of its risk management plan and include the procedures in the standard operating procedures of its contingency plan.

14.0 Standard §164.312(a)(1) Access Control (Required)

Text: "Implement technical policies and procedures for electronic information systems that maintain 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)."

Covered entities must adopt technical means for implementing their information access control policies developed under standard §164.308(a)(4), Information Access Management. The administrative policies and procedures established in Information Access Management under the Administrative Safeguards section of the Security Rule identify and determine the access rights and privileges of authorized users. A covered entity's IT systems must enforce those administrative policies. This standard includes two related mandatory implementation specifications or required components, unique user identification and emergency access procedure, and three addressable implementation specifications, automatic logoff, encryption and decryption, and mechanism to restrict access.

14.1 Implementation Specification §164.312(a)(2)(i) Unique User Identification (Required)

Text: "Assign a unique name and/or number for identifying and tracking user identity."

Each covered entity must assign an identification label to each user specific to that and only that user. System processes will use this label to identify the user and to associate the user with tracked actions

taken by or on behalf of that user. Without unique user identifiers audit logs are not useful in assessing inappropriate access to EPHI by individual users.

14.2 Implementation Specification §164.312(a)(2)(ii) Emergency Access Procedure (Required)

Text: “Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.”

Each covered entity must develop technical procedures, and document instructions, for obtaining EPHI when the normal methods for obtaining access fail because of a crisis situation. Two situations may potentially deny access to patient information stored in automated information systems, including system failure and the unavailability of authorized users. This mandatory implementation specification requires covered entities to develop procedures to grant temporary access to otherwise unauthorized providers when a patient’s authorized providers may not be available (such as, during admission to a hospital Emergency Department). Covered entities should specify procedures for gaining access to information during a system emergency or failure as part of the risk management plan.

14.3 Implementation Specification §164.312(a)(2)(iii) Automatic Logoff (Addressable)

Text: “Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.”

Because this requirement is “addressable”, compliance depends on the outcome of a covered entity’s risk assessment. Covered entities should evaluate the need for, and interval of inactivity that triggers an automatic logoff. A covered entity should determine the need for and the strength of the mechanism of automatic logoff through its risk assessment. A covered entity should also describe and justify its approach to these controls in its risk management plan.

14.4 Implementation Specification §164.312(a)(2)(iv) Encryption and Decryption (Addressable)

Text: “Implement a mechanism to encrypt and decrypt electronic protected health information.”

Because this requirement is “addressable”, compliance depends on the outcome of a covered entity’s risk assessment. This is the first of two times that encryption appears in the final rule and it is important to understand why. The NPRM uses the same general definition each time encryption appears as an addressable implementation specification thus obscuring the differences between the requirements. The differences in meaning become clear only when taken in context with their associated categories and requirements. The final rule changes the wording to put the requirements in context and clarify the rule’s intent. In this specific provision “encryption” is associated with the “Access Control” standard to function as a means of controlling access to protected health information during storage or transmission. Examples of access controlled by this method include encrypting the database or files of sensitive information and encrypting information enroute between a client and server. The risk assessment of each covered entity should determine if encryption of files in storage or transmission is an appropriate method to control access to PHI on their systems based on the nature of the risk, the cost, and their business environment. The covered entity’s risk management plan should describe and justify its approach to this issue.

15.0 Standard §164.312(b) Audit Controls (Required)

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

Covered entities must select and implement a technical service to document system activity. This provision lays the groundwork for the audit requirement found in administrative safeguards. While § 164.308(a)(2)(v) under "Administrative Safeguards" requires covered entities to review the records produced by the audit mechanism, this standard requires covered entities to install and use an audit mechanism. This standard does not state what should be audited. Organizational policies, risk assessments, good industrial practice and other regulations such as the privacy standard determine a covered entity's choice and pattern of auditing events. There are no associated implementation specifications with this standard.

16.0 Standard §164.312(c)(1) Integrity (Required)

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

Covered entities assure data integrity through a combination of many controls including administrative, physical and technical policies and procedures. For example, the administrative policies and procedures for training and information access stipulate that only authorized and trained personnel should review, enter, or modify protected health information. Technical policies and procedures for access control, virus protection, and encryption help protect the integrity of data stored and processed on an automated information system by implementing and enforcing administrative policies in the system. This standard requires covered entities to deploy and use technical policies and procedures to enforce and/or implement all policies and procedures that protect data integrity." There is one addressable implementation specification associated with data integrity, mechanism to authenticate data.

16.1 Implementation Specification §164.312(c)(2) Mechanism to Authenticate Electronic Protected Health Information (Addressable)

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

Because this requirement is "addressable", compliance depends on the outcome of a covered entity's risk assessment. A covered entity must evaluate the need for technical mechanisms to authenticate the integrity of protected health information in its automated information system. A covered entity must describe and justify its approach to this problem in its risk management plan. The proposed rule includes examples of methods such as check sums, message authentication codes, and digital signatures. Inclusion of these examples was not meant to restrict a business' choice of methods to use. Covered entities may deploy other methods of data authentication as long as they provide appropriate levels of data integrity.

17.0 Standard §164.312(d) Person or Entity Authentication (Required)

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

Covered entities must install and use technical procedures that verify the identity of “entities” with access to EPHI. An “entity” in this case includes human users and other machines while transferring or requesting information. Covered entities may use many methods with varying degrees of assurance to satisfy this requirement. As with most of the standards and implementation specifications, the rule does not specify the technology or requisite level of robustness. Covered entities must balance business needs, cost of controls and the sensitivity of the protected information while conducting their risk assessment to determine the robustness of the authentication method. There are no associated implementation specifications.

18.0 Standard §164.312(e)(1) Transmission Security (Required)

Text: “Implement technical security mechanisms to guard against unauthorized access to protected health information that is being transmitted over an electronic communications network.”

This standard requires covered entities to assess and install appropriate technical controls to mitigate threats to data security in transit over all types of networks including but not limited to the Internet, corporate intranets, dedicated lease lines and dial-up connections. Two addressable implementation specifications, “Integrity Controls” and “Encryption” supplement this standard.

18.1 Implementation Specification §164.312(e)(2)(i) Integrity Controls (Addressable)

Text: “Implement security mechanisms to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.”

Because this requirement is “addressable”, compliance depends on the outcome of a covered entity’s risk assessment. Integrity refers to the assurance that a transmitted message arrives at its destination exactly as it left its origin. Data often face increased threat of unauthorized modification during transmission because the entity does not always have control over the transmitting network(s). Most viruses arrive via the Internet presenting another threat to the integrity of data already present in the information system. Covered entities should determine the need for, and type of integrity controls during their organizational risk analyses. Covered entities should also describe and justify their approach to this issue in their risk management plan.

18.2 Implementation Specification §164.312(e)(2)(ii) Encryption (Addressable)

Text: “Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.”

Because this implementation standard is “addressable”, compliance depends on the outcome of a covered entity’s risk assessment. This is the second time that encryption appears in the final rule. In this provision “encryption” appears under the “Transmission Security” standard. Encryption functions as a means of protecting confidentiality and integrity during transmission of a message over a network or other electronic means. If other means cannot effectively protect the data against unauthorized disclosure or modification in the network environment, covered entities should implement encryption as appropriate. This determination should be based on the results of an organization’s risk analysis and explained in its risk management plan. The rule sets no minimum encryption standard.

19.0 Standard §164.314(a)(1) Business associate contracts or other arrangements (Required)

Text: (i) The contract or other arrangement between the covered entity and its business associate required by §164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in §164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful-- (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.

Section §164.314 complements section 308(b) Business Associate Contracts. It states that business associate contracts or memoranda of understanding between government entities must require the business associate to implement administrative, physical and technical safeguards providing a minimum level of protection equivalent to that required by the final rule for security and section §164.502(e) of the Privacy Rule. A covered entity is not in compliance with HIPAA if it knows of breaches of the terms of the agreement by its business associates and takes no action to terminate the contract or report to the Secretary of the Department of Health and Human Services.

19.1 Implementation Specification §164.314(a)(2)(i) Business associate contracts (Required)

Text: "The contract between a covered entity and a business associate must provide that the business associate will-- (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract."

Each covered entity must include the specified elements in their contracts with business associates. The business associate contracts between covered entities and business associates must require the business associate to implement administrative, physical and technical safeguards providing a minimum level of protection equivalent to that required by the final rule for security and section §164.502(e) of the Privacy Rule. The business associate must agree to ensure that any agents or subcontractors to whom it provides information will also implement equivalent safeguards, report any security incidents to the covered entity. The contracts or legal document must allow the covered entity to terminate the contract if the business associate violates the terms of the contract on data security. This ensures that health information that is protected by a provider, health plan or clearinghouse continues to be protected when given to someone that is not required to comply with HIPAA.

19.2 Implementation Specification §164.314(a)(2)(ii) Other arrangements (Required)

Text: "(A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if-- (1) It enters into a memorandum of

understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or (2) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section. (B) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in §160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained. (C) The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by paragraph (a)(2)(i)(D) of this section if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate."

Each covered entity must include the specified elements in their MOU with other government agencies when other law applicable to the business associate that meets the objectives of the specified elements does not exist. This mandatory implementation feature focuses on relations between covered entities and business associates both of which are government entities. Memoranda of Understanding must require the business associate to implement administrative, physical and technical safeguards providing a minimum level of protection equivalent to that required by the final rule for security and section §164.502(e) of the Privacy Rule. The business associate must agree to ensure that any agents or subcontractors to whom it provides information will also implement equivalent safeguards, report any security incidents to the covered entity and make its policies, procedures and related documentation available to the Department of Health and Human Services for determining compliance as needed. The MOU must allow the covered entity to terminate the MOU if the business associate violates the terms of the contract on data security. Governmental agencies may omit the termination clause from the MOU if it is contrary to the legal obligations of the business associate or covered entity. This ensures that health information that is protected by a provider, health plan or clearinghouse continues to be protected when given to someone that is not required to comply with HIPAA.

20.0 Standard §164.314 (b)(1) Requirements for group health plans. (Required)

Text: Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §§164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

Health plans, health insurance companies and HMOs have business needs to disclose some health information to the sponsors of group coverage (i.e. employers). The HIPAA Privacy Rule limits the information health plans may disclose to sponsors and requires the group health plan documents obligate the sponsors to protect and limit the use and disclosure of this health information. The information health plans may disclose to sponsors is limited to summary health information for the purposes of obtaining premium bids from health plans for health insurance coverage, modifying, amending or terminating the plan, and individual information on whether the individual is participating in the plan or is enrolled or

disenrolled in the plan. Required protections include limiting access and preventing use of the information for employment-related actions or decisions or any other employee benefit decisions. This mandatory security standard requires health plan documents provide for the reasonable and appropriate protection of any EPHI disclosed to a plan sponsor.

20.1 §164.314 (b)(2) Implementation Specifications (Required).

Text: The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and (iv) Report to the group health plan any security incident of which it becomes aware.

Each group health plan must have health plan documents that include requirements for a plan sponsor to:

1. implement the same security measures required by the HIPAA Privacy Standard for information it creates, receives, maintains or transmits on behalf of the health plan,
2. ensure that the employees of the sponsor have their duties and access to data separated sufficiently to protect this information from being used for employment or other employee-benefit decisions,
3. require agents of the sponsor to provide reasonable and appropriate protection for health information provided them by the sponsor, and
4. report any security incident of which they become aware to the health plan.

21.0 Standard §164.316 (a) Policies and procedures. (Required)

Text: "A covered entity must, in accordance with §164.306: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart."

This section requires covered entities to implement "reasonable and appropriate" policies and procedures to comply with HIPAA data security standards and implementation specifications. Covered entities must take into account the specific conditions of their individual situation as discussed in the General rules and, thus, ground their approach to HIPAA compliance in risk management. As stated, in deciding which security measures to use, a covered entity must take into account the following factors:

1. The size, complexity, and capabilities of the covered entity.
2. The technical capabilities of record systems used to maintain electronic protected health information.
3. The costs of security measures.
4. The probability and criticality of potential risks to electronic protected health information.

A covered entity cannot try to comply with this standard in a way that breaches requirements of the other HIPAA security standards; but, may change its policies and procedures as long as the changes also do not violate the requirements of the other HIPAA security regulations.

22.0 Standard §164.316(b)(1) Documentation (Required)

Text: A covered entity must, in accordance with §164.306:

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity or assessment.

This standard includes two parts. The first part requires covered entities to document in written format (paper or electronic) policies and procedures pertaining to the protection of electronic protected health information. When organizations develop and maintain their policies and procedures as part of an "oral tradition" only, they become vulnerable to several threats. Orally developed and transmitted policies tend to drift in response to local circumstances thus helping produce varying practice across the organization. In the absence of written rules, organizations inconsistently and incompletely train personnel and find consistent enforcement difficult or impossible. Maintaining policies and procedures in written format safeguards against these threats. The second part requires covered entities to document the results of implementing the policies and procedures when required by a standard or implementation specification. This serves several purposes. Examination of the records for patterns of activity can reveal threats and vulnerabilities, allowing the covered entity to take action to improve the security of protected health information. Because written records demonstrate compliance with policies and procedures, auditors and other surveyors often request to review them during inspections. And finally written records can demonstrate due diligence.

To meet this standard a covered entity must comply with both parts when implementing the standards in the other subparts. For example the implementation specification §164.308(a)(4)(ii) (C) Access Establishment and Modification requires "Ongoing documentation and review of the levels of access to electronic protected health information granted to a user, software program, or procedure." Compliance with the documentation standard dictates that the covered entity must maintain the policies that require the review of the levels of access granted to each user, program or procedure and the procedures followed to conduct those reviews in written or electronic format. They must also maintain the results of each review in a written or electronic format.

This standard makes clear what a covered entity must do to comply. It will be very challenging to create the hierarchy of policies the Security Rule suggests.

22.1 Implementation Specification §164.316(b)(2)(i) Time Limit (Required)

Text: Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

Each covered entity must keep all policies and procedures required by the HIPAA security rule until six years after they are no longer in effect. They must also keep the documented results of actions, activities, assessments, or designations created as a result of the HIPAA security rule for six years. This ensures that the information is available if needed to answer legal questions and other inquiries that might arise.

22.2 Implementation Specification §164.316(b)(2)(ii) Availability (Required)

Text: Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

Each covered entity must make their security documentation available to those who need it. In keeping with the flexible nature of the HIPAA Security Rule, this mandatory implementation specification does not dictate how the covered entity should provide documentation to those who need it. It allows the covered entity to choose methods and intervals that are appropriate to its environment and business structure. Those people with specific security responsibility and users must have access to the written policies and procedures. Ready access to the written procedures improves the likelihood staff will follow them. Covered entities can accomplish this in several ways including, providing offices or individual employees with copies of policy documents and standard operating procedure manuals, training manuals, and web pages.

22.3 Implementation Specification §164.316(b)(2)(iii) Updates (Required)

Text: "Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information."

Each covered entity must keep the policies and procedures current. Changes in the way we do business, upgrades and new equipment and software, new laws and regulations, and a constantly changing threat environment can require changes to policy and operating procedures. Out of date documentation poses a risk to the systems and the information they store and process. A periodic review of those policies and procedures helps to ensure that they are always accurate and appropriate.