

GUIDE TO UNDERSTANDING HIPAA SECURITY
An Instructional Document Written by WorkSmart MD, Inc.
Extracted from the HIPAA Rx™ Compliance Software

On February 20, 2003 the official version of the final security rule was published in the Federal Register. The security rule sets forth security standards that define administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of electronic protected health information (“PHI”).

The final security rule has been narrowed in scope to apply only to health information in electronic form. The Privacy Rule, in contrast, applies to health information in any format, including paper, electronic or oral. The security rule is designed to be technology-neutral and not to mandate specific technology solutions. The security standards are not meant to reflect “best practices” in the information technology security area, but are meant instead to represent a mandated “floor of protection” for electronic PHI. Covered entities have the option to implement security measures that exceed the HIPAA security standards.

Covered entities must document their compliance with the security rule and either make their own “evaluation” of their compliance or obtain a third party “evaluation”. Covered entities also must enter into contractual agreements with their business associates so as to ensure that the business associates will also maintain electronic protected health information received from the covered entities in accordance with the security rule. Covered entities have two years within which to comply with the security rule.

General Rules

Section 164.306(a) provides that covered entities must:

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 the Privacy Rule.
4. Ensure compliance with the security rule by their workforce. DHHS in the preamble refers to the above as the level of risk which is permissible under the security rule. Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementations as specified in the security rule.

In deciding which security measures to use, a covered entity must take into account (1) the size, complexity, and capabilities of the covered entity, (2) the covered entity’s technical infrastructure, hardware, and software security capabilities, (3) the costs of the security measures, and (4) the probability and criticality of potential risks to electronic protected health information. DHHS advises, however, that cost is only one factor to be taken into consideration and is not meant to free covered entities from the responsibility of implementing adequate

security measures.

For any security standard adopted in the security rule that includes “required” implementation specifications, the covered entity must implement the implementation specification. For any security standard that includes “addressable” implementation specifications, the covered entity must assess whether each 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. If the “addressable” implementation specification were determined to be reasonable and appropriate, the entity would implement the specification. If the entity determines that the “addressable” implementation specification is not reasonable and appropriate, the entity would document why it is not implementing the specification and implement an equivalent alternative measure if reasonable and appropriate.

Security measures are divided into three categories of security safeguards:

1. Administrative safeguards
2. Physical safeguards
3. Technical safeguards

In addition, two additional categories of requirements are prescribed: (1) organizational requirements, and (2) policies and procedures and documentation requirements.

Security Standards Matrix

<i>Standards</i>	<i>Sections</i>	<i>Implementation Specifications (R)=Required (A)=Addressable</i>
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)

Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Technical Safeguards		

Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

SECURITY STANDARDS

I. Administrative Safeguards (Section 164.308)

Administrative safeguards are implemented through nine security standards:

(1) Security management process. Implement policies and procedures to prevent, detect, contain and correct security violations. The security management process is the “foundation” of security and is implemented by four “required” implementation specifications:

(a) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI held by the entity.

The depth and scope of risk analysis should be consistent with the type and size of the entity. The following areas should be considered for inclusion:

- Information systems housing PHI
- security processes (security administration, security monitoring, incident response, forensic procedures, and virus detection)
- Physical access to the data center and other critical operations areas
- Contingency planning
- Operating system and/or platform configurations
- Network configurations
- Databases
- Portal/web architecture

Depending on the type and size of the organization, a risk assessment may include internal and external penetration testing, as well as controls around the network and servers/systems that house PHI.

(b) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

The risk management process will include those actions taken to document and mitigate the risks identified in the analysis to a reasonable and appropriate level. The definition of a

reasonable and appropriate level will be left to the discretion of each covered entity, and will be dependent upon size of the entity, level of risk, and cost of safeguard implementation, among others.

(c) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the entity's security policies and procedures.

Covered entities must implement sanction policies for security. The decision as to the type and severity of the sanction imposed will be left to the discretion of each covered entity. The policy should be published as part of the covered entity's security policy, and all employees, vendors, and contractors should be made aware of repercussions of violating the organization's security policies.

(d) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

The intent of this implementation specification is to monitor information system activity through the periodic review of audit logs, access reports, and security incident reports. The degree and scope of implementation will vary depending on the size of the organization. Small healthcare providers may use paper reports to track activities.

(2) Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the required security policies and procedures. Assigned security policy is its own implementation specification, which makes it a "required" implementation specification. The final security rule requires one individual to have accountability for the security procedure of the organization. The organization's Privacy Officer can also be responsible for the entity's compliance with the security rule.

(3) Workforce security. Implement policies and procedures to permit or deny access by the entity's workforce to electronic protected health information, as appropriate. Workforce security is implemented by three "addressable" implementation specifications:

(a) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic PHI or in locations where it might be accessed.

(b) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic PHI is appropriate.

All access to PHI should be assigned based on the need-to-know and job function. Each organization should determine if background employment checks are appropriate prior to allowing an individual access to PHI.

All access to electronic PHI should be documented. To ensure access remains authorized and appropriate, organizations should periodically review access to all electronic PHI.

(c) Termination procedures (Addressable). Implement procedures for terminating access to electronic PHI when the employment of a workforce member ends or as required by workforce clearance procedures.

Covered entities should develop formal termination procedures so that when an employee or contractor is terminated, the following items are addressed:

- Changing of locks/combinations if necessary
- Removal from logical and physical access lists in a timely manner
- Account removal/disablement
- Deletion of personal files
- Return of physical security items (e.g. keys, access card, laptops)

(4) Information access management. Implement policies and procedures for authorizing access to electronic protected health information in conformity with the Privacy Rule. Information access management is implemented by one “required” implementation specification and two “addressable” implementation specifications:

(a) Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic PHI of the clearinghouse from unauthorized access by the larger organization.

(b) Access authorization (Addressable). Implement policies and procedures for granting access to electronic PHI.

Each organization should gather information about current levels of access to corporate applications and applications containing protected health information. If possible, user access to systems should be granted through groups in order to provide the highest level of security.

(c) Access establishment and modification (Addressable). Implement policies and procedures based on the entity’s access authorization policies that establish, document, review and modify a user’s right of access to a workstation, transaction, program or process.

A process to create or modify a user’s system and/or application access must be developed. This process should establish access guidelines that are standardized for all existing applications and systems where possible. This would include items such as:

- Unique identification/authentication with appropriate formats (i.e., not SSN)
- Password management
- Required authorization
- Privileged users (e.g. system administrators and hospital administrators typically require higher levels of access to electronic PHI)

(5) Security awareness and training. Implement security awareness and training for all members of the workforce, including management. Security awareness and training is implemented by four “addressable” implementation specifications:

(a) Security reminders (Addressable). Periodic security updates.

(b) Protection from malicious software (Addressable). Implement procedures for guarding against, detecting and reporting malicious software.

The existence of virus scanning software and virus procedures within an incident response plan should be included in the organization’s overall solution to guard against malicious

software. The intent of the implementation specification is to ensure that there are procedures in place so that all users know how to respond to viruses.

(c) Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

Administrators should monitor log-in attempts from unauthorized users through the examination of audit and log files. Users should be made aware of steps to be taken and who to contact in the event of suspicious scenarios that may include the following:

- User leaves his/her desk and returns to find that he/she has been locked out or cannot login in the morning.
- User notices that a different username has been entered into the log-in box.

(d) Password management (Addressable). Procedures for creating, changing and safeguarding passwords.

All users should be aware of the importance of selecting secure passwords. Secure passwords may include:

- A password that is at least 8 characters long
- A varied set of characters, including lowercase and uppercase letters, numerals, and symbols

(6) Security incident procedures. Implement policies and procedures for addressing security incidents. The security incident procedures standard is implemented by one “required” implementation specification:

(a) Response and reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the entity; and document security incidents and their outcomes.

In the event of a security incident, a covered entity should be able to follow defined policies and procedures for reporting and responding to the security incident. These procedures should include escalation procedures based on the criticality of incident and mitigation for harmful effects.

(7) Contingency plan. Establish and implement emergency response policies and procedures to protect systems which contain electronic protected health information from emergencies and other occurrences, such as fire, vandalism, system failure and natural disaster. Contingency plan is implemented by three “required” implementation specifications and two “addressable” implementation specifications:

(a) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic PHI.

Covered entities should create retrievable exact copies of electronic PHI in the event of an emergency or loss of data. Each organization should perform backups of all systems and information that are required to meet obligations and function successfully.

(b) Disaster recovery plan (Required). Establish, and implement as needed, procedures to restore any loss of data.

This specification specifically requires that covered entities be able to restore any data that has been lost through a disaster. During a disaster, servers and systems may be lost and data will need to be recovered to new systems. Therefore, a disaster recovery plan should be developed for all critical, server-based systems, communications, and infrastructure items (i.e. faxes, e-mail, voicemail). The plan should be periodically reviewed and tested.

(c) Emergency mode operation plan (Required). Establish and implement as needed procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.

PHI will need to be protected, even during a disaster or crisis. For this reason, a crisis management team should be identified that will be responsible for activating the contingency and recovery plans during the emergency mode, coordinating activities and implementing the required tasks. They should be aware of all HIPAA requirements and the location of all PHI.

(d) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

The contingency and recovery plans should be reviewed and tested on a regular basis and should follow every significant change to the business or system/network environment.

(e) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

Information systems, applications, and data groups should be classified according to their criticality and sensitivity.

(8) Evaluation. Perform a periodic technical and non-technical evaluation, based initially upon the standards of the security rule and thereafter in response to changes in the entity's environment or operations affecting the security of electronic PHI, that establishes the extent to which the entity's security policies and procedures meet the requirements of the security rule. The evaluation standard is its own implementation specification, which makes it a "required" implementation specification.

A covered entity's risk analysis and risk management measures must be designed to lead to the implementation of security measures that will comply with the security rule. Each covered entity will be measured not only against its own policies but also against compliance to the HIPAA security standards. This standard is a requirement for each covered entity to evaluate its own security program.

Each covered entity may elect to perform the evaluation on its own or through an external agency or some combination of both. A comprehensive evaluation should at least include the following items:

- Risk analysis
- Threat assessment
- Operating system and network device security configurations
- Workforce security
- Access controls and authorization to PHI
- Security awareness

- Security incident response
- Physical security
- Transmission security
- Security model (i.e., data classification/ownership)
- Security organizational structure
- Security policies/procedures
- Security architecture and design

(9) Business associate contracts and other arrangements. Permit a business associate to create, receive, maintain or transmit electronic PHI on the covered entity’s behalf only if the business associate gives assurances to appropriately safeguard the electronic PHI. This standard has one “required” implementation specification:

(a) Business Associate contract (Required). The covered entity must enter into a business associate contract or other arrangement permitted under Section 164.314(a) that documents the business associate’s assurances to appropriately safeguard the electronic PHI.

Each covered entity should have a clear understanding of what data is being exchanged with its business associates. Each covered entity should clearly document and communicate objectives and responsibilities with regards to protecting electronic PHI to its business associates. The business associate should be able to provide satisfactory assurances that it can and will safeguard all protected health information connected with the covered entity. If it cannot do so, the covered entity may put itself at risk of non-compliance with the HIPAA security standard.

II. Physical Safeguards (Section 164.310)

Physical safeguards are implemented through four security standards:

(1) Facility access controls. Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. This standard is implemented through four “addressable” implementation specifications:

(a) Contingency operations (Addressable). 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.

(b) Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.

This implementation specification should include activities that are related to the securing of a covered entity’s physical facility, such as:

- Performing a walk-through of the building perimeter, interior and any computer room or data center to assess physical security controls and identify control weaknesses.

- Develop a facility security plan that includes physical access procedures during emergency mode operations, periodic testing of the security of the computer room and sensitive areas, and periodic review of the physical access lists.

(c) Access control and validation procedures (Addressable). 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.

This implementation specification should consist of activities related to controlling and validating appropriate access to a physical facility and/or area where PHI is contained. Each covered entity must establish physical security control standards according to the risk in each area and estimated cost for implementing the control. The following items should be considered:

- Procedures for vendors, contractors and visitors access
- Procedures to verify access authorization before granting physical access to a restricted area
- Procedures for security services personnel that include operating procedures during normal business hours, off-hours, and emergency situations

(d) Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security. The term “facility” refers to the physical premises and the interior and exterior of a building.

This implementation specification suggests that facility repairs and modifications be documented and those records be maintained. This may or may not be possible by the covered entity if it resides in a leased facility, but the covered entity could require the building owner to maintain such records.

(2) Workstation use. Implement policies and procedures that specify the proper functions, manner of functioning and the physical attributes of the surroundings of the entity’s workstations that can access electronic PHI. This standard is its own implementation specification, which makes it a “required” implementation specification. The definition of “workstation” includes portable devices, such as laptop computers.

This implementation specification requires the proper use of workstations that contain or have access to PHI. Each covered entity must establish a policy for secure workstation use that includes specific guidelines for both laptop and home system usage. The policy might cover the following topics:

- Encryption of laptops or desktops that contain PHI if physical controls cannot be implemented
- Usage guidelines for covered entity-owned vs. personally-owned home systems
- Virus software protection guidelines
- Software licensing guidelines

(3) Workstation security. Implement physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users. This standard is its own implementation specification, which makes it a “required” implementation specification.

In conjunction with the standard for workstation use, the following topics for workstation security should be considered:

- Require cable locks for all laptops
- Position the screen away from unauthorized users
- Secure in protected areas if possible
- Implement password-protected screen-savers after a specified period of inactivity

(4) Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of the facility and within the facility. This standard is implemented through two “required” implementation specifications and two “addressable” implementation specifications:

(a) Disposal (Required). Implement policies and procedures to address the final disposition of electronic PHI, and/or the hardware or electronic media on which it is stored.

The secure disposal of electronic PHI depends upon properly designed policies for disposal. Within this implementation specification, the covered entity should create a policy and process that includes the following components that address the secure disposal of media and assets that contain electronic PHI:

- Measures to sufficiently erase or overwrite media before disposal
- Additional actions to destroy media (e.g., cutting up floppy disks, where appropriate)
- Measures to appropriately discard media according to the classification level of the data

(b) Media re-use (Required). Implement policies and procedures for removal of electronic PHI from electronic media before the media are made available for re-use.

The covered entity should ensure that there are policies in place to address the secure re-use of media and assets that contain electronic PHI. The covered entity should take the necessary measures to sufficiently erase or overwrite media before re-use (i.e., simply deleting the data is not sufficient).

(c) Accountability (Addressable). Maintain records of the movements of hardware and electronic media and any responsible person therefore.

The covered entity should identify owners for all assets that contain electronic PHI. An inventory of those assets should be maintained, and records of any movement of those assets within or external to the facility should be kept.

(d) Data backup and storage (Addressable). Create retrievable, exact copies of electronic PHI, when needed, before movement of equipment. Removable media devices are not excluded from coverage under this standard.

As part of the Data Backup Plan required under the Contingency Plan, the organization should already be backing up electronic PHI on a routine basis. This item requires an additional safety precaution for the entity to ensure that retrievable, exact copies of electronic PHI are created before movement of any equipment that might cause loss or destruction of data or systems software.

III. Technical Safeguards (Section 164.312)

Technical safeguards are implemented through five security standards:

(1) Access control. Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to authorized persons and programs. This security standard is implemented through two “required” implementation specifications and two “addressable” implementation specifications:

(a) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.

To ensure that users are uniquely identified in an appropriate and controlled manner, the covered entity should develop a framework for completing user profiles or roles for access to existing applications and systems.

(b) Emergency access procedure (Required). Establish and implement as needed procedures for obtaining necessary electronic PHI during an emergency.

As part of the access control procedures, there must be a process to handle logical access to systems and data in emergency situations. The process should include details around the granting emergency access, logging activity during the emergency, return to normal operations (i.e., revocation), and review of emergency access activities.

(c) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

For systems that contain PHI, the covered entity should ensure that mechanisms are in place to terminate sessions after a period of idle time or at the end of the session. Such mechanisms may include:

- A password-protected screen-saver after a period of idle time
- Locking the system when leaving the workstation
- Automatic logoff of the application or network session after a period of idle time

(d) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic PHI.

Based upon the risk analysis, a covered entity should determine if it is necessary to encrypt PHI during transmission or at rest. The use of encryption is a technical and business decision that should be made based on risk. Should the covered entity choose to utilize encryption, encryption and decryption policies and procedures should be developed.

(2) Audit controls. Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI. This security standard is its own implementation specification, which makes it a “required” implementation specification.

Note: Although DHHS supports the use of a risk assessment and risk analysis to determine how intensive any audit control should be, it stresses that audit controls are mandatory. Further, DHHS cautions that the audit controls under the security rule do not satisfy the Privacy Rule’s requirement regarding accounting for disclosures of PHI, since audit trails record uses within an information system, while disclosure accounting applies to disclosures outside of the entity.

Covered entities must implement auditing, logging, and monitoring controls to allow it to examine system activity, both routinely and as result of a possible security incident. Auditing controls may be manual, automatic, or a combination of both. Logs should be reviewed as part of the Information System Activity Review requirement under the security Management Process standard.

Examples of audit controls might include:

- User access and account activity
- Exception reports
- Dormant account reports
- System resource monitoring
- Data integrity controls
- Failed log-in reports

(3) Integrity. Implement policies and procedures to protect electronic PHI from improper alteration or destruction. This security standard is implemented through one “addressable” implementation specification, namely a mechanism to authenticate electronic PHI.

The integrity standard states that mechanisms of the covered entity’s choice should be implemented to ensure that PHI has not been altered or destroyed in any way, whether during transmission or while at rest. There are a number of ways to accomplish this, the most appropriate and practical of which should be determined by the covered entity based on its environment. Some examples include the following:

- Error-correcting memory
- Magnetic disk storage
- Checksums
- Encryption

In addition, policies and procedures should be developed to ensure that PHI is handled appropriately.

(4) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed. This security standard is its own implementation specification, which makes it a “required” implementation specification. Note: DHHS advises that digital signatures and tokens, among other technologies, may be used to implement this standard.

Before granting access to electronic PHI, a process to ensure that a person or entity is who they claim to be must be in place. Authentication is defined as a process utilized by a system to confirm the identity of a user by means of account validation and/or password verification scheme. Each covered entity must develop a mechanism to support and enforce corresponding policies and procedures developed for authentication to PHI. Although no specific implementation is required, examples of procedures for implementing person or entity authentication include the following:

- Username and password
- Token based authentication
- Biometrics
- Challenge and response mechanisms

(5) Transmission security. Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network. This security standard is implemented through two “addressable” implementation specifications:

(a) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of.

This implementation specification implies that controls must be in place to ensure that PHI has not been altered during transmission. The scope of data communications should at least include files transmitted to/from business associates/external entities by FTP, e-mail, dial-up, direct connection, or web access. The covered entity should establish measures for data communications depending on the level of risk based on the method of transmission.

(b) Encryption (Addressable). Implement a mechanism to encrypt electronic PHI whenever deemed appropriate.

NOTE: DHHS advises that there did not yet appear to be available a simple and interoperable solution to encrypting email communications with patients. Therefore, while the proposed security rule made encryption mandatory for transmissions over an “open” network such as the Internet, the final security rule makes the use of encryption and integrity controls an “addressable” implementation specification. Where the risk of interception is “significant”, DHHS expects the entity to encrypt the transmission, if appropriate, under the “addressable” implementation specification.

ADDITIONAL REQUIREMENTS

I. Organizational Requirements (Section 164.314)

Organizational requirements are implemented through two standards:

(1) Business associate contracts or other arrangements, which requires a covered entity to take reasonable steps to cure a business associate’s material breach or violation of the business associate contract if the covered entity knew of a pattern of activity or practice of the business associate which constituted such material breach or violation. If the reasonable steps are unsuccessful, the covered entity must either terminate the business associate contract or report the problem to the Secretary of DHHS, if termination is infeasible. This standard has one “required” implementation specification, which involves the use of a business associate contract or other arrangement. Note: The “chain of trust” agreement of the proposed security rule has been replaced with the business associate contract. The final security rule also makes the health component and affiliated entity standards of the Privacy Rule applicable to the security rule, so as to require the covered entity to protect the electronic PHI from unauthorized access by the larger organization of which it is a part. The business associate contract must provide that the business associate will:

- (a) Implement safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic PHI that it creates, receives, maintains or transmits on behalf of the covered entity.
- (b) Ensure that any agent, including a subcontractor, to whom it provides this information
- (c) agrees to implement reasonable and appropriate safeguards.
- (d) Report to the covered entity any security incident of which it becomes aware.
- (e) Authorize termination of the business associate contract by the covered entity if the covered entity determines that the business associate has violated a material term of the contract. In addition, in the preamble DHHS advises that the business associate agreement must provide that the business associate will make its policies and procedures, and required documentation relating to the safeguards, available to the Secretary of DHHS for purposes of determining the covered entity's compliance with the security rule. The covered entity may require the business associate to meet higher security standards than the "floor" contained in the security rule. If the covered entity and its business associate are both governmental entities, an "other arrangement" is sufficient, permitting the entities to alter the form of their agreement to conform to statutory requirements.

II. Policies and Procedures and Documentation Requirements (Section 164.316)

Policies and procedures and documentation requirements are implemented through two standards:

(1) Policies and procedures. Covered entities are required to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of the security rule. This standard is its own implementation specification, which makes it a "required" implementation specification.

(2) Documentation. Covered entities are required to maintain written documentation (which may be electronic) of the implemented policies and procedures and of any action, activity or assessment which is required to be documented. Three "required" implementation specifications relate to this standard.

(a) Time limit (Required). Covered entities are required to retain the documentation required under the above standard for six years from the date of its creation or the date when it last was in effect, whichever is later.

(b) Availability (Required). Covered entities must make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(c) Updates (Required). Covered entities must review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic PHI.