HIPAA SECURITY RULE

Published February 20, 2003 – See Federal Register Vol. 68, No. 34 pp. 8334-8381
Compliance Date April 20, 2005

The Security Rule requires administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of electronic protected health information (PHI). The Security Rule requires covered entities to implement detailed safeguards to protect electronic PHI from unauthorized access, alteration, deletion, and transmission.

For assistance in complying with the HIPAA Security Regulations, the Medical Society has entered into an agreement with PrivaPlan who has developed a program that will help physicians comply with the complex security regulations. As part of the agreement, PrivaPlan will offer a significant discount to MSSNY members. For more information on PrivaPlan and to obtain the MSSNY member code go to the Members Only section of the MSSNY website or call Mary Rush at 488-6100 ex 411.

The Privacy Rule applies to PHI in any form. The Security Rule applies to PHI in electronic form.

General Requirement – Ensure "CIA"

Confidentiality – only the right people see it;

Integrity – No unauthorized alteration or deletion;

Availability – the right people can see it when needed.

A covered entity must protect against reasonably anticipated hazards to the security or integrity of PHI

Protect against reasonably anticipated uses and disclosures not permitted by the Privacy Rule.

Ensure compliance by workforce.

The Security Rule applies to all electronic PHI the covered entity creates, receives, maintains, or transmits. The scope of the Security Rule is more limited than the scope of the Privacy Rule. The Privacy Rule applies to PHI in any form, whereas the Security Rule applies only to PHI in electronic form.

Scalability/Flexibility – In deciding which security measures to use a covered entity may take into account factors such as:

- Size, complexity and capabilities of the covered entity;

– Technical infrastructure, hardware and software security capabilities;

– Cost of security measures;

– Probability and criticality of potential risks to electronic PHI.

Technologically Neutral – The Security Rule defines what a covered entity must do but does not prescribe any specific technology covered entities must use. Technology is constantly changing, so the rule does not prescribe any specific technology.

In addition to adopting Standards the Rule adopts Implementation Specifications that provide instructions for implementing those standards.

Required vs. Addressable - The Security Rule establishes two types of implementation specifications: “Required” and “Addressable”. Required implementations must be met. With respect to an addressable implementation, the covered entity must assess whether an implementation specification is a reasonable and appropriate safeguard in its environment, which may include consideration of factors such as the size and capability of the organization as well as the risk. If the organization determines it is a reasonable and appropriate safeguard, it must implement the specification. If an addressable implementation specification is determined not to be a reasonable and appropriate answer to the covered entity’s security needs, the covered entity must do one of two things: implement another equivalent measure if reasonable and appropriate, or if not determined to be reasonable and appropriate, do not implement.

The covered entity must document the rationale for not implementing the implementation specification.

ADDRESSABLE DOES NOT MEAN OPTIONAL. ADDRESSABLE REQUIRES ASSESSMENT AND DOCUMENTATION.

The symbol “R” refers to a Required specification. “A” refers to an Addressable specification.

164.308 Administrative Safeguards

164.308(a)(1)(i) Standard: Security Management Process - Implement policies and procedures to prevent, detect, contain and correct security violations.

Implementation Specifications

- ❑ (ii)(A) Risk Analysis (R) - Conduct an assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of PHI held by the covered entity;

- ❑ (ii)(B) Risk Management (R) – Implement Security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level;

- ❑ (ii)(C) Sanction Policy (R) – Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity;

- ❑ (ii)(D) Information System Activity Review (R) – Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

164.308(a)(2) Standard: Assigned Security Responsibility (R) – Identify the security official who is responsible for the development and implementation of the policies and procedures required for the entity.

The standard requires that the final responsibility for a covered entity's security must be assigned to one official. More than one individual may be given specific security responsibilities. However, a single individual must be designated as having the overall final responsibility for the security of PHI.

[Comment – Getting Started – The first step is to perform a Risk Analysis. A Risk Analysis must be conducted before completing security policies and procedures.

For discussion of Risk Analysis see:

WEDI/SNIP http://snip.wedi.org/
NIST http://csrc.nist.gov/publications/drafts.htm/

Assemble a Security Compliance Team. A team should include the Security Official and may include other individuals, such as: someone familiar with the entity's electronic systems (IT staff), office manager, someone responsible for overseeing medical records, billing staff, regulatory/legal representative, privacy officer (if different than Security Official), physician manager.

A Risk Analysis is not an IT issue only. There are Technical and Administrative aspects. IT staff may be needed to analyze technical aspects. Administrative and managerial representation is needed for administrative aspects, such as budgetary decisions.]

164.308(a)(3)(i) Standard: Workforce Security – Implement policies and procedures to ensure that all members of the workforce have appropriate access to electronic PHI and to prevent those workforce members who do not have access from obtaining access to PHI.

Implementation Specifications

- ❑ (ii)(A) Authorization and/or Supervision (A) – Implement procedures for the authorization and/or supervision of workforce members who work with electronic PHI or in locations where it might be accessed.

- □ (ii)(B) Workforce Clearance Procedure (A) – Implement procedures to determine that the access of a workforce member to electronic PHI is appropriate.

- □ (ii)(C) Termination Procedures (A) - Implement procedures for terminating access to electronic PHI when the employment of a workforce member ends. (These features would include such things as changing combination locks, removal from access list, removal of user account(s), and the turning in of keys, tokens, or cards that allow access).

164.308(a)(4)(i) Standard: Information Access Management – Implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of the [Privacy Rule].

Implementation Specifications

- □ (ii(A) Isolating Health Care Clearinghouse Functions (R); [pertains to health care clearinghouse, not addressed in this summary].

- □ (ii)(B) Access Authorization(A) – Implement policies and procedures for granting access to electronic PHI, for example, through access to a workstation, transaction, program, process, or other mechanism;

- □ (ii)(C) Access Establishment and Modification(A) – 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.

164.308(a)(5)(i) Standard: Security Awareness and Training – Implement a security awareness and training program for all workforce members (including management).

Implementation Specifications

- □ (ii)(A) Security Reminders (A); Periodic Security updates;

- □ (ii)(B) Protection from Malicious Software (A) Procedures for guarding against, detecting, and reporting malicious software (virus protection);

- □ (ii)(C) Log-in Monitoring (A) Procedures for monitoring log-in attempts and reporting discrepancies;

- □ (ii)(D) Password Management (A) Procedures for creating, changing, and safeguarding passwords.

164.308(a)(6)(i) Standard: Security Incident Procedures - Implement policies and procedures to address security incidents.

Implementation Specifications

- □ (ii) Response and Reporting (R) - 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.

“Security Incident” is defined at 164.304 as “… the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system”.

164.308(a)(7)(i) Standard: Contingency Plan - 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 PHI.

Implementation Specifications

- □ (ii)(A) Data Backup Plan (R) – Establish and implement procedures to create and maintain retrievable exact copies of electronic PHI;

- □ (ii)(B) Disaster Recovery Plan (R) – Establish (and implement as needed) procedures to restore any loss of data;

- □ (ii)(C) Emergency Mode Operation Plan (R) – 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;

- □ (ii)(D) Testing and Revision Procedures (A) – Implement procedures for periodic testing and revision of contingency plans;

- □ (ii)(E) Applications and Data Criticality Analysis (A) – Assess the relative criticality of specific applications and data in support of other contingency plan components.

164.308(a)(8) Standard: Evaluation (R) - Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic PHI, that establishes the extent to which an entity’s security policies and procedures meet the [Security Requirements].

[Evaluation may be performed either internally by entity’s own workforce or may be external, depending upon the covered entity. An external evaluation may be too costly for small entities, preamble page 8351].

164.308(b)(1) – Standard: Business Associate Contracts and Other Arrangements. A covered entity may permit a business associate to create, receive, maintain, or transmit electronic PHI 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.

Implementation Specifications

(b)(4) Written contract or other arrangement (R). The covered entity must document the satisfactory assurances through a written contract or other arrangement that satisfies 164.314(a).

164.314(a) – Business Associate Contract.

(i) The contract between the covered entity and the 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 PHI that it creates, receives, maintains or transmits on behalf of covered entity as required by [the Security Rule].
>
> B. Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguard 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.

164.314(a)(ii) address "other arrangements".

164.314(a)(ii)(A) pertains to other arrangements that apply when the covered entity and the business associate are both government entities [not addressed in this summary].

164.314(a)(ii)(B) pertains to situation where a business associate is required by law to perform a function or activity on behalf of the covered entity [not addressed in this summary].

164.310 Physical Safeguards

164.310(a)(1) Standard: Facility Access Controls - 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.

Implementation Specifications

- ❑ (2)(i) Contingency Operations (A) - 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.

- ❑ 2(ii) Facility Security Plan (A) - Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.

[The covered entity retains the responsibility for addressing facility security even where it shares space within a building with other organizations. Facility security measures taken by a third party must be considered and documented in the covered entity's facility security plan, where appropriate].

- ❑ (2)(iii) Access Control and Validation Procedures (A) - 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.
- ❑ (2)(iv) Maintenance Records (A) - Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

164.310(b) Standard: Workstation Use (R) - 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 workstation that can access electronic PHI.

[Instructions/procedures delineating the proper functions to be performed and the manner in which these functions can be performed; e.g. logging off before leaving a workstation unattended].

164.310(c) Standard: Workstation Security (R) - Implement physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users.

164.310(d)(1) Standard: 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 the movement of these items within the facility.

Implementation Specifications

- ❑ (2)(i) Disposal (R). Implement policies and procedures to address the final disposition of electronic PHI, and/or hardware or electronic media on which it is stored.
- ❑ (2)(ii) Media Re-use (R). Implement procedures for removal of electronic PHI from electronic media before media are made available for re-use.
- ❑ (2)(iii) Accountability (A). Maintain a record of the movements of hardware and electronic media and any person responsible therefor.

  [This requires a record of the actions of a person relative to the receipt and removal of hardware and/or software into and out of a facility that are traceable to that person; e.g. the appropriate mechanism for a given entity may be a manual, such as receipt and removal restricted to specific persons, with logs kept.]

- □ (2)(iv) Data Backup and Storage (A) - Create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment.

164.312 Technical Safeguards

164.312(a)(i) Standard: Access Control – Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights as specified in [Information Access Management].

Implementation Safeguards

- □ (2)(i) Unique User Identification (R) - Assign a unique name and/or number for identifying and tracking user identity (e.g., user name password);

- □ 2(ii) Emergency Access Procedure (R) - Establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency;

- □ 2(iii) Automatic Log Off (A) - Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity;

- □ Encryption and Decryption (A) - Implement a mechanism to encrypt and decrypt electronic PHI.

164.312(b) Standard: Audit Controls (R) - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

[Entities have flexibility to implement the standard in a manner appropriate to their needs as deemed necessary by their own risk analysis. For example, see NIST Special Publication 800-14. Generally, Accepted Principles and Practices for Securing Information Technology Systems and NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security].

164.312(c)(1) Standard: Integrity - Implement policies and procedures to protect electronic PHI from improper alteration or destruction.

Implementation Specifications

- □ (c)(2) Mechanism to authenticate electronic PHI (A). Implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an authorized manner.

[Error correcting memory and magnetic disc storage are examples of the built-in data authentication mechanisms in hardware and operating systems. Preamble p. 8356]

164.312(d) Standard: Person or Entity Authentication (R) - Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed.

> [Covered entities may use whatever mechanism is reasonable and appropriate. “Digital signatures” and “soft tokens” are examples listed in the preamble, page 8356].

164.312(e)(1) Standard: Transmission Security - Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network.

Implementation Specifications

- ❑ (2)(i) Integrity Controls (A) - Implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of;

- ❑ (2)(ii) Encryption (A) - Implement a mechanisms to encrypt electronic PHI whenever deemed appropriate.

[Preamble page 8357 states, particularly when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting e-mail communications with patients. As a result, encryption is an Addressable implementation. The Centers for Medicare and Medicaid Services, however, encourages that providers consider the use of encryption technology for transmitting electronic PHI, particularly over the internet].

164.314 Organizational Requirements

164.314(a)(i) Business Associate Contracts or other arrangements; see 164.308(b)(i)

If the covered entity knows of a pattern of activity or practice of the business associate that constitutes a material breach or violation of the business associate’s obligation under the business associate contract, the covered entity must take reasonable steps to cure the breach. If such steps are unsuccessful, the covered entity must terminate the contract. If termination of the contract is not feasible, the covered entity must report the problem to HHS.

164.314(b) Requirements for group health plans [not addressed in this summary].

164.316 Standard: Policies and Procedures and Documentation Requirements

The Security Rule requires covered entities to implement policies and procedures that are reasonably designed, taking into account the size and type of activities of the covered entity that relate to electronic PHI (scalability), and requires that the policies and procedures be DOCUMENTED in written form, which may be in electronic form. A covered entity may change its policies and procedures at any time, provided that it documents it.

Implementation Specifications

- ❑ (b)(2)(i) Time Limit (R) - Retain the documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
- ❑ (b)(2)(ii) Availability (R) - Make the documentation available to those persons responsible for implementing the procedures.
- ❑ (b)(2)(ii) Updates (R) - Review documentation periodically, and update as needed, in response to environmental or operational changes.

Where to Get Help

http://www.cms.hhs.govhipaa/hipaa2/ - CMS HIPAA Administrative Simplification Website for Electronic Transactions and Code Sets, Security, and Unique Identifiers

HHS http://aspe.hhs.gov/adminsimp/
OCR www.hhs.gov/ocr/hipaa
WEDI/SNIP http://snip.wedi.org/
NIST http://csrc.nist.gov/publications/drafts.html

CMS Hotline: 866-282-0659
AskHIPAA@cms.hhs.gov

Filename:	HIPAASEC RULE
Directory:	U:\Website\HIPAA
Template:	C:\Documents and Settings\jyate\Application Data\Microsoft\Templates\Normal.dot
Title:	HIPAA SECURITY RULE
Subject:	
Author:	Joan Capoua
Keywords:	
Comments:	
Creation Date:	10/6/2004 11:26 AM
Change Number:	5
Last Saved On:	11/30/2004 11:27 AM
Last Saved By:	MSSNY
Total Editing Time:	42 Minutes
Last Printed On:	11/30/2004 11:27 AM
As of Last Complete Printing	
Number of Pages:	10
Number of Words:	3,107 (approx.)
Number of Characters:	19,052 (approx.)