SUMMARY OF

HIPAA FINAL SECURITY RULE

INTRODUCTION

On February 20, 2003, the Department of Health and Human Services ("HHS") published the final HIPAA security standards, *Health Insurance Reform: Security Standards; Final Rule, 45 CFR Parts 160, 162 and 164, 68 Fed. Reg. 8333*. These standards establish a security management framework for the protection of Electronic Protected Health Information (EPHI). Significantly, this final Security Rule applies only to protected health information in electronic form and, unlike the earlier Privacy Rule, does not cover paper copies of documents or oral information. The standards established in the Security Rule are necessarily intertwined with the requirements of the Privacy Rule. Specifically, the Privacy Rule requires the use of reasonable administrative, physical and technical safeguards to protect privacy, and the new Security Rule provides guidance for interpreting the reasonableness of such safeguards. Most covered entities must be in compliance with the Security Rule by April 21, 2005.

General Rule

Generally, the Security Rule requires a covered entity to:

1) Ensure the confidentiality, integrity, and availability of all EPHI 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; and
4) Ensure compliance by its workforce.

45 C.F.R. § 164.306(a). The Security Rule offers flexibility in how a covered entity chooses to meet the above security requirements, allowing consideration of such factors as the cost of a particular security measure, the size of the covered entity involved, the complexity of the approach, the technical infrastructure and other security capabilities in place, and the nature and scope of potential security risks. Rather than requiring specific technical measures, the Security Rule takes a goal-oriented approach, establishing "standards" that all covered entities must meet, accompanied by implementation specifications to guide compliance with each standard.

The implementation specifications are divided into two categories: required and addressable. Covered entities must implement all required implementation specifications, which are security measures that HHS has deemed fundamental to any reasonable security compliance program. For addressable implementation specifications, however, a covered entity must assess the reasonableness and appropriateness of each specification in the context of its own security framework. In making this assessment, a covered entity may consider a variety of factors, including "the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation." When considering an addressable implementation specification, therefore, a covered entity may determine that:

- a particular addressable implementation specification is reasonable and appropriate, in which case it must implement such addressable implementation specification;

- a particular addressable implementation specification is unreasonable or inappropriate, but that the given security standard cannot be met without implementing an additional security safeguard, in which case the covered entity may implement an alternate measure that accomplishes the same end, provided it documents the decision not to implement the addressable implementation specification, the rationale behind that decision, and the alternative safeguard implemented to meet the standard; or

- a particular implementation specification is simply not applicable and no additional measures are necessary to meet the given standard, in which case the covered entity must document the decision not to implement the addressable specification, the rationale behind that decision, and how the standard is being met.

Standards

The Security Rule identifies three categories of standards: administrative, physical and technical. Administrative safeguards primarily address the policies and procedures a covered entity must have in place to document its ability to insure the confidentiality, integrity and availability of EPHI. There are nine administrative security standards, including Security Management Process, Assigned Security Responsibility, Workforce Security, Information Access Management, Security Awareness and Training, Security Incident Procedures, Contingency Plan, Evaluation, and Business Associate Contracts and Other Arrangements. To meet these standards, a covered entity must implement required implementation specifications, including, among others, Risk Analysis, Risk Management, Information System Activity Review, Response and Reporting, Data Backup, Disaster Recovery, and Emergency Mode Operation. There are also important addressable implementation specifications, including, among others, Authorization and/or Supervision, Workforce Clearance Procedures, Termination Procedures, Access Authorization, Protection from Malicious Software, and Password Management.

Physical safeguards focus on the physical security measures in place to secure EPHI. The applicable standards are Facility Access Controls, Workstation Use, Workstation Security, and Device and Media Controls. The required implementation specifications include, among others, Disposal and Media Re-use, and the addressable implementation specifications include Contingency Operations, Facility Security Plan, Access Control and Validation Procedures, Maintenance Records, Accountability, and Data Backup and Storage.

Finally, the technical safeguards detail the standards for access control, auditing, user authentication and the other technical measures involved in securing stored and transmitted EPHI. Technical safeguards include five standards, among which are Access Controls, Audit Controls, Integrity, Person or Entity Authentication, and Transmission Security. The required implementation specifications include Unique User Identification and Emergency Access Procedures, and among the addressable implementation specifications are Automatic Logoff, Encryption and Decryption, Mechanisms to Authenticate EPHI, and Integrity Controls. For a complete list of the standards and implementation specifications, please refer to the attached chart.

Business Associate Agreements

Like the Privacy Rule, the Security Rule embraces the concept of business associate agreements, requiring covered entities to enter into agreements with business associates who create, receive, maintain or transmit EPHI on their behalf. Under such agreements, the business associate must:

- implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the covered entity's electronic protected health information;

- ensure that its agents and subcontractors to whom it provides the information do the same; and

- report to the covered entity any security incident of which it becomes aware.

The contract must also authorize termination if the covered entity determines that the business associate has violated a material term. As under the Privacy Rule, a covered entity is not liable for violations by the business associate unless the covered entity knew that the business associate was engaged in a practice or pattern of activity that violated HIPAA, and the covered entity failed to take corrective action.

Getting Started

Compliance with the Security Rule is a significant undertaking and will likely take at least several months of planning and implementation. Initial steps in HIPAA Security Rule implementation include:

- Identify team (including designation of a Security Officer) to analyze, implement and manage security compliance;

- Establish a workplan and timeline;

- Determine whether you need outside consulting or legal assistance to help with HIPAA Security Rule implementation;

- Inventory EPHI to determine where it is maintained and travels and inventory administrative, physical and technical security measures currently in place;

- Perform a comprehensive risk assessment to identify, categorize and quantify security risks and vulnerabilities;

- Analyze each Security Rule standard and implementation specification in light of the results of the risk assessment;

- Develop appropriate security policies and deploy any needed technology.

HIPAA SECURITY STANDARDS

ADMINISTRATIVE SAFEGUARDS

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

PHYSICAL SAFEGUARDS

Standards	Sections	Implementation Specifications (R) Required, (A) = Addressable	
Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)		(R)
Workstation Security	164.310(c)		(R)
Device and Media Controls	164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

TECHNICAL SAFEGUARDS

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

HIPAA SECURITY STANDARDS AND IMPLEMENTATION SPECIFICATION(S)		
STANDARDS (In Bold) AND IMPLEMENTATION SPECIFICATION(S)	*	**BRIEF EXPLANATION**
Security Management Process:		Implement policies and procedures to prevent, detect, contain and correct security violations.
➢ Risk Analysis	R	
➢ Risk Management	R	
➢ Sanction Policy	R	
➢ Information System Activity Review	R	
Assigned Security Responsibility	R	Identify the security official who is responsible for the development and implementation of the policies and procedures required by the Security Rule.
Workforce Security:		Implement policies and procedures to ensure that all personnel have appropriate access levels to EPHI.
➢ Authorization and/or Supervision	A	
➢ Workforce Clearance Procedure	A	
➢ Termination Procedures	A	
Information Access Management		Implement policies and procedures for authorizing access to EPHI consistent with sound IT practices and the Security Rule.
➢ Access Authorization	A	
➢ Access Establishment & Modification	A	
Security Awareness & Training		Implement a security awareness and training program for all personnel (including management).
➢ Security Reminders	A	
➢ Protection from Malicious Software	A	
➢ Log-in Monitoring	A	
➢ Password Management	A	
Security Incident Procedures		Implement policies and procedures to address security incidents.
➢ Response and Reporting	R	
Contingency Plan		Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, or natural disaster) impacting systems with EPHI.
➢ Data Backup Plan	R	
➢ Disaster Recovery Plan	R	
➢ Emergency Mode Operation Plan	R	
➢ Testing Revision Procedures	A	
➢ Applications & Data Criticality Analysis	A	
Evaluation of Security Policies: ➢ Periodic Technical & Non-Technical Evaluation	R	Perform a periodic technical and non-technical evaluation (based on the standards in the Security Rule and in response to environmental and operational changes) to determine whether then-current security policies and procedures comply with the requirements of the Security Rule.
Business Associate Contracts & Other Arrangements ➢ Written Contract or Other Arrangement	R	Covered Entities may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the Covered Entity obtains certain assurances specified in the Security Rule.
Facility Access Controls		Implement policies and procedures to restrict physical access to electronic information systems and the facility or facilities in which they are housed to properly authorized personnel only.
➢ Contingency Operations	A	
➢ Facility Security Plan	A	
➢ Access Control & Validation Procedures	A	
➢ Maintenance Records	A	
Workstation Use	R	Implement policies and procedures specifying the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations permitted to access EPHI.
Workstation Security	R	Implement physical safeguards for all workstations that access EPHI to restrict access to authorized users.
Device and Media Controls:		Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.
➢ Disposal	R	
➢ Media Re-Use	R	
➢ Accountability	A	
➢ Data Backup & Storage	A	
Access Controls:		Implement technical policies and procedures for information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights.
➢ Unique User Identification	R	
➢ Emergency Access Procedure	R	
➢ Automatic Logoff	A	
➢ Encryption & Decryption	A	
Audit Controls	R	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.
Integrity		Implement policies and procedures to protect EPHI from improper alteration or destruction.
➢ Mechanism to Authenticate EPHI	A	
Person or Entity Authentication	R	Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.
Transmission Security		Implement technical security measures to guard against unauthorized access to EPHI being transmitted over a network.
➢ Integrity Controls	A	
➢ Encryption	A	