

HIPAA Security

July 16, 2004

HIPAA and Other Security

Topic	HIPAA	The Bigger Picture
Needs to protect...	Electronic PHI	All information; financial, personnel, strategic, etc.
Attitude	"Is it in the rule?"	"Does it make good business sense?"
Compliance	April 2005	On-going
Penalties	\$100 per violation (Civil) \$50,000 - \$250,000 (Criminal)	\$150,000 for each program copied illegally Up to \$250,000 (Criminal)

HIPAA Security Standards

- Administrative Safeguards (55%)
 - 12 Required, 11 Addressable
- Physical Safeguards (24%)
 - 4 Required, 6 Addressable
- Technical Safeguards (21%)
 - 4 Requirements, 5 Addressable

Administrative Safeguards

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

Physical Safeguards

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

Technical Safeguards

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

Risk Assessment and Analysis

Each covered entity:

- Assesses its own security risks
- Determines its risk tolerance or risk aversion
- Devises, implements, and maintains appropriate security to address its business requirements
 - Does not imply that organizations are given complete discretion to make their own rules
- Documents its security decisions

Electronic Protected Health Information (ePHI)

- ePHI is Protected Health Information (individually identifiable health information that is created, maintained, transmitted or received by a HIPAA covered entity) that is in electronic form, both at rest on any electronic media as well as in transit over any type of network, private or public.

Information Security Program

1. Assess and analyze risks
2. Develop policies and procedures to address the risks
3. Select and implement cost-effective controls, countermeasures and safeguards
4. Train the workforce on their responsibilities
5. Manage the computing environment
6. Audit, monitor and respond to incidents