

HIPAA Security Regulations - An Overview

Administrative Safeguards			
Standards	CFR 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)	<i>none</i>	(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 Healthcare 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)	<i>none</i>	(R)
Business Associate Contracts	164.308(b)(1)	Written Contract or Other Arrangement	(R)

Physical Safeguards			
Standards	CFR 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)	<i>none</i>	(R)
Workstation Security	164.310(c)	<i>none</i>	(R)
Device and Media Controls	164.310(d)(1)	Media Disposal	(R)
		Media Re-use	(R)
		Media Accountability	(A)
		Data Backup and Storage (during transfer)	(A)

Technical Safeguards			
Standards	CFR 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 (data at rest)	(A)
Audit Controls	164.312(b)	<i>none</i>	(R)
Integrity	164.312(c)(1)	Protection Against Improper Alteration or Destruction of Data	(A)
Person or Entity Authentication	164.312(d)	<i>none</i>	(R)
Transmission Security	164.312(e)(1)	Integrity Controls	(A)
		Encryption (FTP and Email over Internet)	(A)