HIPAA Security Rule Auditor Checklist

12/12/2018 7:53

Standard	CFR Sections	Implementation Specifications (R)=Required (A)=Addressable	In Compliance	References	Issues
Administrative Safeguards					
Security Management Process	**164.308(a) (1)**				
Risk Analysis		(R)	Yes	HIPAA Risk Analysis	
Risk Management		(R)	Yes	HIPAA Management Plan	
Sanction Policy		(R)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Information System Activity Review		(R)	Yes	HIPAA Policy and Procedures, Login History by Computer Report	
Assigned Security Responsibility	**164.308(a)(2)**				
		(R)	Yes	HIPAA Policy and Procedures, HIPAA Evidence of Compliance	
Workforce Security	**164.308(a)(3)**				
Authorization and/or Supervision		(A)	No	HIPAA Policy and Procedures, HIPAA Evidence of Compliance, User Identification Worksheet, Network Share Identification Worksheet	See HIPAA Management Plan
Workforce Clearance Procedure		(A)	N/A	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	
Termination Procedures		(A)	Yes	HIPAA Policy and Procedures, HIPAA Evidence of Compliance, User Identification Worksheet	
Information Access Management	**164.308(a)(4)**				
Isolating Health care Clearinghouse Function		(R)	N/A		
Access Authorization		(A)	No	HIPAA Policy and Procedures, HIPAA Evidence of Compliance, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Access Establishment and Modification		(A)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Security Awareness and Training	**164.308(a)(5)**				
Security Reminders		(A)	N/A	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	
Protection from Malicious Software		(A)	No	HIPAA Policy and Procedures, HIPAA Evidence of Compliance	See HIPAA Management Plan
Log-in Monitoring		(A)	Yes	Login History Report, HIPAA Policy and Procedures	
Password Management		(A)	No	HIPAA Policy and Procedures, HIPAA Evidence of Compliance	See HIPAA Management Plan
Security Incident Procedures	**164.308(a)(6)**				
Response and Reporting		(R)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Contingency Plan	**164.308(a)(7)**				

Data Backup Plan		(R)	Yes	HIPAA Policy and Procedures, HIPAA Evidence of Compliance	
Disaster Recovery Plan		(R)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Emergency Mode Operation Plan		(R)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Testing and Revision Procedure		(A)	Yes	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	
Applications and Data Criticality Analysis		(A)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Evaluation	**164.308(a)(8)**				
Evaluation		(R)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Business Associate Contracts	**164.308(b)(1)**				
Written Contracts or Other Arrangements		(R)	No	HIPAA Policy and Procedures, HIPAA Evidence of Compliance	See HIPAA Management Plan
Physical Safeguards					
Facility Access Controls	**164.310(a)(1)**				
Contingency Operations		(A)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Facility Security Plan		(A)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Access Control and Validation Procedures	**No**	(A)	N/A	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	
Maintenance Records		(A)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Workstation Use	**164.310(b)**				
Workstation Use		(R)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Workstation Security	**164.310(c)**				
Workstation Security		(R)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Device and Media Controls	**164.310(d)(1)**				
Media Disposal		(R)	Yes	HIPAA Policy and Procedures, HIPAA Evidence of Compliance, HIPAA Policy and Procedures Validation Worksheet	
Media Re-use		(R)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Media Accountability		(A)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Data Backup and Storage (during transfer)		(A)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Technical Safeguards					
Access Control	**164.312(a)(1)**				
Unique User Identification		(R)	No	HIPAA Policy and Procedures, HIPAA Evidence of Compliance	See HIPAA Management Plan
Emergency Access Procedure		(R)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Automatic Log off		(A)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan

Encryption and Decryption (data at rest)		(A)	Yes	HIPAA Policy and Procedures, HIPAA Evidence of Compliance, Drive Encryption Report	
Audit Controls	**164.312(b)**				
Audit Controls		(R)	No	HIPAA Policy and Procedures, HIPAA Evidence of Compliance	See HIPAA Management Plan
Integrity	**164.312(c)(1)**				
Protection Against Improper Alteration or Destruction of Data		(A)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Person or Entity Authentication	**164.312(d)**				
Person or Entity Authentication		(R)	No	HIPAA Policy and Procedures, HIPAA Evidence of Compliance	See HIPAA Management Plan
Transmission Security	**164.312(e)(1)**				
Integrity Controls		(A)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Encryption (FTP and Email over Internet)		(A)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan