HIPAA Auditor Checklist

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)	No	HIPAA Policy and Procedures, HIPAA Evidence of Compliance, User Identification Worksheet	See HIPAA Management Plan
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)	Yes	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	
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)	Yes	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	
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)	Yes	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	
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)	Yes	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	
Facility Security Plan		(A)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Access Control and Validation Procedures	**Yes**	(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)	Yes	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	
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)	Yes	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	
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)	Yes	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	
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)	Yes	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	
Encryption (FTP and Email over Internet)		(A)	No	HIPAA Policy and Procedures, HIPAA Policy and Procedures Validation Worksheet	See HIPAA Management Plan
Privacy Rule					
Notice of Privacy Practices	**45 CFR § 164.520**				
Missing Notice of Privacy Practices Policy			No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
Missing Evidence - Notice of Privacy Practices Policy			Yes	HIPAA Privacy Rule Worksheet	
Notice of Privacy Practices Incorrect Wording			Yes	HIPAA Privacy Rule Worksheet	
Missing Evidence - Notice of Privacy Practices			No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
Notice of Privacy Practices Not Given to all New Patients			Yes	HIPAA Privacy Rule Worksheet	
Notice of Privacy Practices Acknowledgement Received from all New Patients			Yes	HIPAA Privacy Rule Worksheet	
Missing Evidence - Notice of Privacy Practices Acknowledgement Form			Yes	HIPAA Privacy Rule Worksheet	
Notice of Privacy Practices Not Available Upon Request			Yes	HIPAA Privacy Rule Worksheet	
Notice of Privacy Practices Not Posted in Patient Area			Yes	HIPAA Privacy Rule Worksheet	
Missing Evidence - Notice of Privacy Practices - Displayed in Patient Areas			Yes	HIPAA Privacy Rule Worksheet	
Notice of Privacy Practices Not Prominently Displayed on Website			No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
Missing Evidence - Notice of Privacy Practices - Prominently Displayed on Website			Yes	HIPAA Privacy Rule Worksheet	
Notice of Privacy Practices - Training			Yes	HIPAA Privacy Rule Worksheet	
Patient's Right to Access Records	**45 CFR § 164.524**				
No written Patient's Right to Access Records Policy			No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
Missing Evidence - Patient's Right to Access Records Policy & Procedures			Yes	HIPAA Privacy Rule Worksheet	
Fees for medical records not consistent with HIPAA and other regulations			Yes	HIPAA Privacy Rule Worksheet	
Patient's Right to Access Records Deadline			Yes	HIPAA Privacy Rule Worksheet	
Patient's Right to Access Mental Health Records			Yes	HIPAA Privacy Rule Worksheet	
Patient's Right to Access Records - What to Provide			Yes	HIPAA Privacy Rule Worksheet	
Patient's Right to Access Records - Deceased Individuals			Yes	HIPAA Privacy Rule Worksheet	
Missing Law Enforcement, Court Orders and Subpoenas Policy			Yes	HIPAA Privacy Rule Worksheet	
Missing Evidence - Law Enforcement, Court Orders and Subpoenas Policy			No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
Law Enforcement, Court Orders and Subpoenas - Training			No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
Missing Evidence - Law Enforcement, Court Orders and Subpoenas - Training			Yes	HIPAA Privacy Rule Worksheet	
Marketing	**45 C.F.R. § 164.501, 45 CFR § 164.508(a)(3)**				
No HIPAA-related Marketing Policy			Yes	HIPAA Privacy Rule Worksheet	
Missing Evidence - HIPAA-related Marketing Policy			No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
No HIPAA-related Marketing Policy Training			No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
Missing Evidence - HIPAA-related Marketing Policy Training			Yes	HIPAA Privacy Rule Worksheet	
Minimum Necessary Access	**45 CFR § 164.502(b), 45 CFR § 164.514(d)**				
No Minimum Necessary Access Policy			Yes	HIPAA Privacy Rule Worksheet	
Missing Evidence - Minimum Necessary Access Policy.			No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
No Minimum Necessary Access Training			No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
Missing Evidence - Minimum Necessary Access Training			Yes	HIPAA Privacy Rule Worksheet	
No Minimum Necessary Access Internal Auditing			Yes	HIPAA Privacy Rule Worksheet	
Missing Evidence - Minimum Necessary Access Internal Auditing			No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
Confidential Communications	**45 C.F.R. § 164.502(h), 45 C.F.R. § 164.522(b)**				
No Confidential Communications Policy			No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
Missing Evidence - Confidential Communications Policy			Yes	HIPAA Privacy Rule Worksheet	

No Confidential Communications Training		Yes	HIPAA Privacy Rule Worksheet	
Missing Evidence - Confidential Communications Training		Yes	HIPAA Privacy Rule Worksheet	
No Confidential Communications Documentation		Yes	HIPAA Privacy Rule Worksheet	
No Confidential Communications Systems/Processes		Yes	HIPAA Privacy Rule Worksheet	
Business Associates	**45 CFR § 164.502(e), § 164.504(e), § 164.532(d) and (e)**			
Missing Business Associates Policy		Yes	HIPAA Privacy Rule Worksheet	
Missing Evidence - Business Associates Policy		No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
No Training on Business Associates		No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
Missing Evidence - Training on Business Associates		Yes	HIPAA Privacy Rule Worksheet	
Missing Business Associates Agreements		Yes	HIPAA Privacy Rule Worksheet	
Authorizations for Uses & Disclosures	**45 CFR § 164.508**			
Authorizations for Uses & Disclosures		No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
Missing Evidence - Authorizations for Uses & Disclosures		Yes	HIPAA Privacy Rule Worksheet	
No Authorizations for Uses & Disclosures Training		Yes	HIPAA Privacy Rule Worksheet	
Missing Evidence - Authorizations for Uses & Disclosures Training		Yes	HIPAA Privacy Rule Worksheet	
Missing Authorizations for Uses & Disclosures Forms		Yes	HIPAA Privacy Rule Worksheet	
Uses & Disclosures – Emergencies & Disasters	**45 CFR §164.510(b)(4)**			
Uses & Disclosures - Emergencies & Disasters		Yes	HIPAA Privacy Rule Worksheet	
Missing Evidence - Uses & Disclosures - Emergencies & Disasters		No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
No training on Uses & Disclosures - Emergencies & Disasters		No	HIPAA Privacy Rule Worksheet	See HIPAA Management Plan
Missing Evidence - Uses & Disclosures - Emergencies & Disasters Training		Yes	HIPAA Privacy Rule Worksheet	
Uses & Disclosures – Mental and Behavioral Health, including Opioid Overdose	**45 CFR 164.510(b)**			
Missing Policy and Procedures for Uses & Disclosures - Mental and Behavioral Health, including Opioid Overdose		Yes	HIPAA Privacy Rule Worksheet	
No training in Uses & Disclosures - Mental and Behavioral Health, including Opioid Overdose.		Yes	HIPAA Privacy Rule Worksheet	
Breach Notification Rule				
Breach Complaint & Determination	**45 CFR § 164.414(a), § 164.530(i)**			
Missing Breach Complaint and Determination Policy		Yes	HIPAA Breach Notification Rule Worksheet	
Missing Evidence - Breach Complaint and Determination Policy		Yes	HIPAA Breach Notification Rule Worksheet	
Breach Complaint and Determination Training		No	HIPAA Breach Notification Rule Worksheet	See HIPAA Management Plan
Missing Evidence - Breach Complaint and Determination Training		Yes	HIPAA Breach Notification Rule Worksheet	
Breach Risk Assessment	**45 CFR § 164.402, § 164.530(i)**			
Missing Breach Risk Assessment Policy		Yes	HIPAA Breach Notification Rule Worksheet	
Missing Evidence - Breach Risk Assessment Policy		No	HIPAA Breach Notification Rule Worksheet	See HIPAA Management Plan
Breach Risk Assessment Training		No	HIPAA Breach Notification Rule Worksheet	See HIPAA Management Plan
Missing Evidence - Breach Risk Assessment Training		Yes	HIPAA Breach Notification Rule Worksheet	
Individual Notification	**45 CFR § 164.404**			
Missing Breach Individual Notification Policy		Yes	HIPAA Breach Notification Rule Worksheet	
Missing Evidence - Breach Individual Notification Policy		No	HIPAA Breach Notification Rule Worksheet	See HIPAA Management Plan
Breach Individual Notification Training		No	HIPAA Breach Notification Rule Worksheet	See HIPAA Management Plan
Missing Evidence - Breach Individual Notification Training		Yes	HIPAA Breach Notification Rule Worksheet	
Regulatory Reporting	**45 CFR § 164.408**			
Missing Breach Reporting Policy		Yes	HIPAA Breach Notification Rule Worksheet	
Missing Evidence - Breach Reporting Policy		No	HIPAA Breach Notification Rule Worksheet	See HIPAA Management Plan
Breach Reporting Training		No	HIPAA Breach Notification Rule Worksheet	See HIPAA Management Plan
Missing Evidence - Breach Reporting Training		Yes	HIPAA Breach Notification Rule Worksheet	