HIPAA AUDIT CHECKLIST

Checklist Category	Document Name/Description	Received Y/N	Document/File Name(s)
General Information			
General Information	Complete the enclosed "HIPAA Privacy and Security Performance Audit Survey"		
General Information	Any previous audit reports, evaluations or assessments of HIPAA Privacy and Security Rules and Breach Notification Rule		
General Information	Please confirm whether your organization uses or discloses PHI in: • Fundraising activities; or • Research activities		
HIPAA Security			
General Governance – HIPAA Security	Identify any applicable industry guidance (e.g., studies, practices, regulations, etc…) or other reference material used to develop any of the policies and procedures requested below (NO NEED TO PROVIDE THIS DCUMENTATION - SIMPLY IDENTIFY)		
General Governance – HIPAA Security	Security Officer contact information (name, email, phone, address and admin contact info)		
Administrative Safeguards	Entity-Level Risk Assessment		
Administrative Safeguards	Risk assessments for systems that house ePHI		
Administrative Safeguards	Risk Management Policy		
Administrative Safeguards	Organizational Chart		
Administrative Safeguards	Information Security Policies, specifically those documenting security management practices and processes, such as: • Access Control • Data Protection • Acceptable Use • Workstation Security • Workforce/HR Security • Sanction Procedures		

Checklist Category	Document Name/Description	Received Y/N	Document/File Name(s)
HIPAA Security Cont'd			
Administrative Safeguards	Security Incident Management Plan		
Administrative Safeguards	Business Continuity/Disaster Recovery Plan		
Administrative Safeguards	Most recent Disaster Recovery Exercise Documentation		
Administrative Safeguards	Data backup and recovery procedures		
Physical Safeguards	Physical Security Policies and Procedures		
Physical Safeguards	Data Destruction and Media Reuse Procedure		
Physical Safeguards	List of roles based access - job level and level of PHI access needed for function; log of employees based on their PHI access type		
Technical Safeguards	Encryption Policies and Procedures		
Technical Safeguards	Management's internal control/internal audit policies and procedures related to monitoring IT safeguards		
Technical Safeguards	System-generated user access listing of all individuals with access to systems housing PHI		
Technical Safeguards	System-generated listing of all new hires within the past year		
Technical Safeguards	User Authentication Policies and Procedures		
HIPAA Privacy			
General Governance – HIPAA Privacy	Identify any applicable industry guidance (e.g., studies, practices, regulations, etc…) or other reference materials used to develop any of the policies and procedures requested below (NO NEED TO PROIVDE THIS DOCUMENTATION – SIMPLY IDENTIFY)		
General Governance – HIPAA Privacy	Compliance/Privacy Officer contact information (name, email, phone, address and admin contact info)		
HIPAA Privacy	Privacy Policy(ies) and Notice of Privacy Practices		

Checklist Category	Document Name/Description	Received Y/N	Document/File Name(s)
HIPAA Privacy Cont'd			
HIPAA Privacy	Privacy practices documentation including: • Use and disclosure • Right to request privacy information • Right to request privacy protection of PHI • Individual access to PHI • Denial access to PHI procedures • Amendment of PHI • Accounting of disclosures of PHI • Administrative requirements		
HIPAA Privacy	Training documentation of employees over privacy practices and organization training policy(ies)		
HIPAA Privacy	Policies and procedures in place over administrative, technical and physical safeguards covering all forms of PHI		
HIPAA Privacy	Complaints handling policies and procedures		
HIPAA Privacy	Population of complaints over privacy practices made with the last year (complaint log)		
HIPAA Privacy	Sanction and disciplinary policies and procedures over privacy violations		
HIPAA Privacy	Mitigation and disciplinary policies and procedures when a breach occurs		
HIPAA Privacy	Anti-intimidation/anti-retaliation policies and procedures		

Checklist Category	Document Name/Description	Received Y/N	Document/File Name(s)
HIPAA Privacy Cont'd			
HIPAA Privacy	Policies and procedures over uses and disclosures of PHI, including: • Deceased individuals • Personal representatives • Confidential communication • Business associate contract requirements • Health plan documentation requirements • Treatment, payment, and/or operations • Consent and authorization requirements • Judicial or administrative proceeding requirements • Research requirements • Approval and waiver requirements • De-identification/Re-identification of PHI procedures • PHI procedures • Restriction of PHI • Minimum necessary requirements • Limited information provided for fundraising purposes • Health care underwriting • Identity verification procedures of individuals requesting PHI		
HITECH Organizational Process-Based Capabilities			
HITECH	Breach notification process, entity-level risk assessment documentation and capabilities		