HIPAA

This checklist is intended to assist hospitals, physician practices, and other provider "covered entities" in complying with The Health Insurance Portability and Accountability Act of 1996 (HIPAA). Refer to https://www.hhs.gov/hipaa/index.html for the most current rules and guidance.

Patients	Yes	No
Do patients have immediate access to clinical information in compliance with the Cures Act?	☐	☐
Is there a process for patients requesting amendments to medical records?	☐	☐
Is there a process for patients requesting restrictions on specific uses and disclosures?	☐	☐
Are patients able to receive confidential communications of PHI "by alternative means or at alternative locations" if requested?	☐	☐
Are patients able to receive an accounting of disclosures of PHI to third parties if requested?	☐	☐
Are patients instructed on how to file a complaint about HIPAA privacy violations?	☐	☐
Is there a process for allowing patients to inspect and copy medical records?	☐	☐
Is your Notice of Privacy Practices (NPP) kept current, HIPAA compliant, provided to patients at least annually, copies available for patients, and posted in a prominent location?	☐	☐
Have you designated in writing someone who is responsible for receiving complaints about privacy and who is able to answer questions about your NPP?	☐	☐
Do you document all complaints received, as well as how they were resolved?	☐	☐
Other: Specify		

Disclosures	Yes	No
Is the "minimum necessary" standard applied to all access to and disclosures of PHI?	☐	☐
Are separate authorizations obtained for disclosures of psychotherapy notes, substance use disorders, and HIV status (if required) according to federal and state laws?	☐	☐

Do your disclosure policies adequately address disclosures that may be permissible without patient consent, such as treatment, payment, operations, law enforcement, adult and child protective services, and public health, in accordance with state and federal laws?	☐	☐
Is a disclosure log maintained according to HIPAA requirements, including patient consent/authorization where applicable?	☐	☐
Other: Specify		

Physical Environment/Security	Yes	No
Is PHI only accessible to authorized personnel?	☐	☐
Are computer displays with PHI facing away from patients/visitors?	☐	☐
Do all buildings and sensitive areas within the buildings have restricted access?	☐	☐
Do patient registration, exam, and consultation rooms provide adequate privacy?	☐	☐
Are all computers password protected and time out when inactive?	☐	☐
Are medical charts outside of exam rooms turned inward to hide information?	☐	☐
Do you govern the receipt and removal of hardware and electronic media that contain ePHI into and out of your facilities, as well as the movement of these items within your facilities?	☐	☐
Do you implement a mechanism to encrypt and decrypt ePHI?	☐	☐
Do you implement procedures for creating, changing, and safeguarding passwords?	☐	☐
Do you have procedures for guarding against, detecting, and reporting malicious software?	☐	☐
Do all computer users log off when they physically leave their workstations?	☐	☐
Do you require all PHI to be encrypted when shared across public networks?	☐	☐
Other: Specify		

Personnel	Yes	No
Have you assigned a designated staff member as the HIPAA Compliance, Privacy, and/or Security Officer?	☐	☐
Have you trained all employees on basic HIPAA requirements?	☐	☐
Do you conduct training for all employees, including management, to keep them current on your updated P&P, and is this training documented?	☐	☐

Have you documented all HIPAA training?	☐	☐
Is employee access to PHI role-based and limited to what is necessary to perform their job functions?	☐	☐
When an employee leaves your organization or has a change in responsibilities, do you terminate their access to ePHI or limit/expand their access as appropriate?	☐	☐
Other: Specify		

Policies/Procedures/Agreements	Yes	No
Do you have policies and procedures that address HIPAA Privacy Rule requirements?	☐	☐
Do you have policies and procedures that address HIPAA Security Rule requirements?	☐	☐
Do you have policies and procedures that address HIPAA Enforcement Rule requirements?	☐	☐
Do you have policies and procedures that address HIPAA Breach Notification Rule requirements?	☐	☐
Have you identified all business associates?	☐	☐
Do you have up-to-date written contracts with your Business Associates (BA Agreements) that meet all current HIPAA requirements?	☐	☐
Have you communicated security and privacy policies and procedures to all employees?	☐	☐
Have you documented annual review of policies and procedures?	☐	☐
Other: Specify		

Security Incidences/Breaches	Yes	No
Do you have policies and procedures in place to account for and document any PHI violations?	☐	☐
Do you have policies and procedures in place to notify the appropriate parties in the event of a breach?	☐	☐
Do you implement procedures to identify and respond as needed to suspected or known security incidents, including breaches of unsecured PHI?	☐	☐
Have you implemented a process for employees to anonymously report a HIPAA violation?	☐	☐
Do you have a contingency plan in place for responding to an emergency that damages systems or physical locations containing PHI?	☐	☐

Have you created a system to track and manage violation investigations?	☐	☐
Are processes in place to provide breach information in the timeframe described by HHS?	☐	☐
Are you reporting breach violations with fewer than 500 individuals to the HHS annually?	☐	☐
Other: Specify		

Audits/ Risk Assessments	Yes	No
Have you conducted a security risk assessment?	☐	☐
Have you conducted a privacy assessment?	☐	☐
Have you conducted an administrative assessment?	☐	☐
Have you identified all deficiencies discovered during the audits?	☐	☐
Have you documented all deficiencies?	☐	☐
Have you audited your business associates to ensure they are HIPAA compliant?	☐	☐
Have you created a remediation plan for deficiencies found in the security risk assessment?	☐	☐
Have you created a remediation plan for deficiencies found in the privacy assessment?	☐	☐
Have you created a remediation plan for deficiencies found in the administrative assessment?	☐	☐
Other: Specify		

Print Save