HIPAA Compliance Checklist

The HHS' Office for Civil Rights has identified the following area to be essential elements of an effective HIPAA compliance program. How does your organization fare?

Use the checkboxes below to self-evaluate HIPAA compliance in your practice or organization.

- ☐ **The following six annual audits/assessments are required elements of a HIPAA compliance program. Have they been completed?**
  - ☐ Security Risk Assessment
  - ☐ Privacy Assessment (Not required for BAs)
  - ☐ HITECH Subtitle D Audit
  - ☐ Security Standards Audit
  - ☐ Asset and Device Audit
  - ☐ Physical Site Audit
- ☐ **Do you have documentation to show you have conducted the above audits/assessments for the past six years?**
- ☐ **Have you identified all gaps uncovered in the audits above?**
  - ☐ Have you documented all deficiencies?
- ☐ **Have you created remediation plans to address deficiencies found in all six audits?**
  - ☐ Are these remediation plans fully documented in writing?
  - ☐ Do you update and review these remediation plans annually?
  - ☐ Are annually documented remediation plans retained in your records for six years?
- ☐ **Have all staff members undergone annual HIPAA training?**
  - ☐ Do you have documentation to confirm each employee has completed their annual training?
  - ☐ Is there a staff member designated as the HIPAA Compliance, Privacy, and/or Security Officer?
- ☐ **Have all staff members received Security Awareness training?**
  - ☐ Do you have documentation to confirm each member of the workforce has completed their security awareness training?
  - ☐ Do you provide periodic reminders to reinforce security awareness training?
- ☐ **Have you developed a contingency plan for emergencies?**
  - ☐ Have you developed policies and procedures for responding to emergency situations?
  - ☐ Are you creating backups of all ePHI to ensure an exact copy can be recovered in the event of a disaster?
  - ☐ Have you developed procedures to ensure critical business processes continue when operating in emergency mode?
  - ☐ Are your contingency plans regularly updated and tested?

- ☐ **Have you, by means of a risk analysis, assessed whether encryption of ePHI is appropriate?**
  - ☐ If encryption is not appropriate, have you implemented alternative and equivalent measures to ensure the confidentiality, integrity, and availability of ePHI?
  - ☐ Have you implemented controls to guard against unauthorized accessing of ePHI during electronic transmission?
  - ☐ Has the decision-making process covering the use of encryption been documented?

- ☐ **Have you implemented identity management and access controls?**
  - ☐ Have you assigned unique usernames/numbers to all individuals who require access to ePHI?
  - ☐ Is access to ePHI restricted to individuals that require access to perform essential work duties?
  - ☐ Have you implemented policies and procedures for assessing whether employees' access to ePHI is appropriate?
  - ☐ Have you developed policies and procedures for terminating access to ePHI when an employee leaves an organization or their role changes?
  - ☐ Do you have policies for recovering all electronic devices containing ePHI when an employee leaves your organization?
  - ☐ Does your system automatically logout a user after a period of inactivity?

- ☐ **Do you create and monitor ePHI access logs?**
  - ☐ Are auditable ePHI access logs created for successful and unsuccessful login attempts?
  - ☐ Are ePHI access logs routinely monitored to identify unauthorized accessing of ePHI?
  - ☐ Have you implemented controls to ensure ePHI cannot be altered or destroyed in an unauthorized manner?

- ☐ **Are all permitted uses and disclosures of PHI/ePHI limited to the minimum necessary information to achieve the purpose for which the PHI/ePHI is disclosed?**

- ☐ **Have you developed policies and procedures covering the secure disposal of protected health information and electronic PHI?**
  - ☐ Have you developed policies and procedures for rendering physical PHI unreadable, indecipherable, an incapable of being reconstructed when no longer required?
  - ☐ Have you developed policies and procedures for permanently erasing ePHI on electronic devices when they are no longer required, or the devices reach end of life?
  - ☐ Are electronic devices containing ePHI and physical PHI stored securely until they are disposed of in a secure fashion?

- ☐ **Have you developed policies and procedures for providing patients with access to their health information?**
  - ☐ Are you providing individuals with access to their health information or copies of their health information on request?
  - ☐ Are you providing copies of PHI in the format requested by the individual?
  - ☐ Are you providing individuals copies of their health information in a timely manner and within 30 days?
  - ☐ If fees are charged, are those fees reasonable and cost-based?

- ☐ **Do you obtain and store HIPAA authorizations for uses and disclosures of PHI not otherwise permitted by the HIPAA Privacy Rule?**
  - ☐ Do your authorizations clearly explain the specific uses and disclosures of PHI and are they written in plain language?
  - ☐ Do your authorizations state the classes of people to whom PHI will be disclosed?
  - ☐ Do the authorizations include an expiry date or event?
  - ☐ Do the authorizations contain the individual's signature and date of signature?

- ☐ **Have you created a Notice of Privacy Practices (NPP)?**
  - ☐ Do you provide periodic reminders to reinforce security awareness training?
  - ☐ Have you provided your notice of privacy practices to all patients?
  - ☐ Has every patient stated in writing that they have received the notice of privacy practices?
  - ☐ Has your notice of privacy practices been published in a prominent location and on your website?
  - ☐ Have you developed procedures for dealing with complaints about failures to comply with the NPP?

- ☐ **Do you have policies and procedures relevant to the annual HIPAA Privacy, Security, and Breach Notification Rules?**
  - ☐ Have all staff members read and legally attested to the HIPAA policies and procedures?
  - ☐ Do you have documentation of their legal attestation?
  - ☐ Do you have documentation for annual reviews of your policies and procedures?

- ☐ **Have you identified all of your vendors and business associates?**
  - ☐ Do you have Business Associate Agreements (BAAs) in place with all business associates?
  - ☐ Have you performed due diligence on your business associates to assess their HIPAA compliance?
  - ☐ Are you tracking and reviewing your Business Associate Agreements annually?
  - ☐ Do you have Confidentiality Agreements with non-business associate vendors?

- ☐ **Do you have a defined process for security incidents and data breaches?**
  - ☐ Do you have the ability to track and manage the investigations of all incidents?
  - ☐ Are you able to provide the required reporting of minor or meaningful breaches or incidents?
  - ☐ Do your staff members have the ability to anonymously report a privacy/security incident or potential HIPAA violation?

Disclaimer - Always consult an expert.

This checklist is composed of general questions about the measures your organization should have in place to ensure HIPAA compliance, and does not qualify as legal advice. Successfully completing this checklist does not guarantee that you or your organization are HIPAA compliant. You should always consult a HIPAA compliance expert.