

HIPAA Compliance Checklist

The following questions represent the core components necessary for HIPAA compliance. Please check off as applicable to self-evaluate your practice or organization. This does not take the place of a Risk Assessment and should not be considered legal advice.

- Have you conducted the following Audits/Assessments?**
 - Security Risk Assessment
 - Privacy Assessment
 - Administrative Assessment

- Have you identified all deficiencies discovered during the audits?**
 - Have you documented all deficiencies?

 - Are documents readily available in the event of a HIPAA audit?

- Have you created remediation plans to address deficiencies for the following?**
 - Security Risk Assessment
 - Privacy Assessment
 - Administrative Assessment

- Do you have Policies and Procedures relevant to the HIPAA Privacy, Security, and Breach Notification Rules?**
 - Have all staff members been trained on HIPAA Policies and Procedures?
 - Do you have documentation of their attestation?
 - Do you have documentation for annual reviews of your Policies and Procedures?

- Have all staff members undergone basic HIPAA training?**
 - Do you have documentation of their training?
 - Is there a staff member designated as the HIPAA Compliance, Privacy, and/or Security Officer?

- Have you identified all Business Associates?**
 - Do you have Business Associate Agreements in place with all Business Associates?
 - Do they have BAAs in place with their subcontractors/vendors that work with your practice?
 - Have you audited your Business Associates to ensure that they are HIPAA compliant?
 - Do you have reporting to prove your due diligence?

- Do you have a management process in the event of incidents or breaches?**
 - Can you track and manage the investigation of all incidents?
 - Are you able to demonstrate that you have investigated each incident?
 - Are you able to provide reporting of minor or meaningful breaches or incidents?
 - Can your staff members anonymously report an incident?