

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.

☐ **Have you conducted the following 6 required annual Audits/Assessments?**

- | | |
|---|---|
| ☐ Security Risk Assessment | ☐ Security Standards Audit |
| ☐ Privacy Assessment | ☐ Asset and Device Audit |
| ☐ HITECH Subtitle D Audit | ☐ Physical Site Audit |

☐ **Have you identified all gaps uncovered in the audits above?**

- ☐ Have you documented all deficiencies?

☐ **Have you created remediation plans to address deficiencies for the following?**

- | | |
|---|---|
| ☐ Security Risk Assessment | ☐ Security Standards Audit |
| ☐ Privacy Assessment | ☐ Asset and Device Audit |
| ☐ HITECH Subtitle D Audit | ☐ Physical Site Audit |

☐ **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 Policies and Procedures?
- ☐ Do you have documentation of their legal attestation?
- ☐ Do you have documentation for annual reviews of your Policies and Procedures?

☐ **Have all staff members undergone annual 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 (and Confidentiality Vendors? New box?)**

- ☐ Do you have Business Associate Agreements in place with all Business Associates?
- ☐ Have you audited your Business Associates to ensure that they are HIPAA compliant?
- ☐ Are you tracking and reviewing your Business Associate Agreements annually?
- ☐ Do you have Confidentiality Agreements with those who are not considered Business Associates?

☐ **Do you have a defined process in the event of incidents or 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 an incident?

AUDIT TIP: If audited, you must provide all documentation in an eligible format to auditors.

*This checklist is composed of general questions about the measures your organization should have in place to state that you are HIPAA compliant, and does not qualify as legal advice. Successfully completing this checklist **DOES NOT** certify that you or your organization are HIPAA compliant.*