

HIPAA Compliance Checklist

*The following are identified by HHS OCR as elements of an effective compliance program.
Please check off as applicable to self-evaluate your practice or organization.*

Have you conducted risk assessments for the following areas in the last year?

- Data Security
- Privacy Standards (Not required for BAs)
- Breach Determination and Notification Requirements

Have you identified all gaps uncovered in the assessments above?

- Have you documented all the gaps and deficiencies?

Have you created a corrective action plan to address these identified gaps?

- Is this plan fully documented in writing?
- Do you update and review this plan annually?
- Do you have plan in place to manage and retain your reports, findings and records for six (6) years?

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?

Do you have adopted Policies and Procedures relevant to the 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 you identified all of your vendors and Business Associates?

- Do you have Business Associate Agreements 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 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 for the past six (6) years to auditors.**

*Need help completing your Checklist? Schedule your HIPAA consultation today
at (929) 492-2234 info@compliancegroup.com*

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.

