

# HIPAA Compliance Questionnaire



Below are questions that cover the core essential components necessary for a HIPAA compliant organization. Please check the answers that apply to your organization to quickly evaluate your practice or organization.

- ☐ **Have you conducted the following Audits/Assessments? (NIST Guidelines)**
  - ☐ Security Risk Assessment
  - ☐ Privacy Assessment
  - ☐ Administrative Assessment
- ☐ **Have you Identified all deficiencies discovered during the audits?**
  - ☐ Have you documented all deficiencies?
- ☐ **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 read and attested to the 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?
  - ☐ 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?**
  - ☐ Do you have the ability to track and manage the investigations 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?
  - ☐ Do your staff members have the ability to anonymously report an incident?

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

**HIPAA compliance does not have to be complicated.  
Centerpoint IT can make sure you have a plan for HIPAA compliance.  
Contact us at (404) 781-0200 or [info@centerpointIT.com](mailto:info@centerpointIT.com).**

This HIPAA questionnaire serves as a guide with basic questions about your practice's HIPAA readiness and areas that must be addressed to be HIPAA compliant. This questionnaire does not represent legal advice but serves only as a guide to HIPAA readiness. A more thorough engagement is required to analyze and ensure your technology systems and procedures comply with recommended HIPAA best practices.

© 2018 Centerpoint IT | Private & Confidential

