

HIPAA Compliance Checklist

Can You Check Everything Off?

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

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.



Need help completing your Checklist?

Speak with a Compliance Expert at

801-610-6000
or
support@911it.com

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?

- ☐ All deficiencies are documented.

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

- ☐ They are fully documented in writing.
- ☐ I update and review these remediation plans annually.
- ☐ Annually documented plans are retained in my records for six (6) years.

Have all staff members undergone annual HIPAA training?

- ☐ I have documentation of their training.
- ☐ There is a staff member designated as the HIPAA Compliance, Privacy, and/or Security Officer.

Do you have Policies and Procedures relevant to the annual HIPAA Privacy, Security, and Breach Notification Rules?

- ☐ All staff members have read and legally attested to the Policies and Procedures.
- ☐ Employee legal attestations are documented.
- ☐ Policies and Procedures are reviewed annually, and it's documented.

Have you identified all of your vendors and Business Associates?

- ☐ I have Business Associate Agreements in place with all Business Associates.
- ☐ I have performed due diligence on my Business Associates to assess their HIPAA compliance.
- ☐ I am tracking and reviewing my Business Associate Agreements annually.
- ☐ I have Confidentiality Agreements with non-Business Associate vendors.

Do you have a defined process for incidents or breaches?

- ☐ I have the ability to track and manage the investigations of all incidents.
- ☐ I am able to provide the required reporting of minor or meaningful breaches or incidents.
- ☐ My 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.