SCALE community

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 selfevaluate 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.

**AUDIT TIP: If audited, you must provide all documentation for the past six (6) years to auditors.*

Have you conducted the following six (6) required annual Audits/Assessments?

- ☐ Security Risk Assessment
- ☐ Privacy Standards Audit (Not required for BAs)
- ☐ HITECH Subtitle D Privacy Audit
- ☐ Security Standards Audit
- ☐ Asset and Device Audit
- ☐ Physical Site Audit

Have you identified all gaps uncovered in the audits above?

- ☐ All deficiencies are documented.

Have you created remediation plans to address deficiencies found in all six (6) Audits?

- ☐ They are fully documented in writing.
- ☐ I update and review these remediation plans annually.
- ☐ Annually documented remediation 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.

SCALE community

SCALE prides itself in developing customized solutions for its clients and helping healthcare organizations grow and thrive in a challenging marketplace. Now, we are ready to help you. We look forward to sharing examples of how we have helped our clients and invite you to schedule a 1-on-1 complimentary practice management consultation with us.

Need help completing your Checklist? Contact Roy Bejarano at roy@scale-healthcare.com, or +1 (917) 428-0377.