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 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?

- ❏ Have you documented all deficiencies?

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

- ❏ Are these remediation plans fully documented in writing?
- ❏ Do you update and review these remediation plans annually?
- ❏ Are annually documented remediation plans retained in your 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 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 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.