HIPAA Compliance Checklist

☐ Have you conducted the following six required annual Audits/Assessments?

- ☐ Security Risk Assessment (Annually)
- ☐ Privacy Assessment
- ☐ HITECH Subtitle D Audit
- ☐ Security Standards Assessment
- ☐ Asset and Device Audit
- ☐ Physical Site Assessment

☐ 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 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 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 Policy 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 mange 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?