GLBA Compliance Checklist for 2026

Documentation Requirements

- ☐ Written information security program approved by the board or governing body
- ☐ Designated Qualified Individual responsible for the security program
- ☐ Written risk assessment identifying internal and external threats to customer information
- ☐ Incident response plan with defined roles, escalation procedures, and communication protocols
- ☐ Written vendor management policy covering security requirements for service providers
- ☐ Documentation of all material changes to systems, operations, or business arrangements
- ☐ Board-level reporting from the Qualified Individual at least annually

Testing and Monitoring Items to Include in Your GLBA Checklist

- ☐ Annual penetration testing covering all systems that store, process, or transmit NPI
- ☐ Vulnerability assessments conducted at least every six months
- ☐ Continuous monitoring program or documented justification for periodic testing approach
- ☐ Penetration test scoping aligned with current risk assessment findings
- ☐ Remediation tracking: documented fixes for all critical and high-severity findings
- ☐ Retesting of remediated vulnerabilities within 60 to 90 days
- ☐ Testing triggered by material changes to infrastructure, applications, or business operations
- ☐ Evidence that penetration testing is human-driven and goes beyond automated scanning

Required Updates to Your Security Program

- ☐ Access controls reviewed and updated based on risk assessment findings
- ☐ Encryption implemented for customer information in transit and at rest
- ☐ Multi-factor authentication deployed for all users accessing customer information
- ☐ Secure development practices documented and followed for in-house applications
- ☐ Data retention and disposal procedures reviewed and enforced
- ☐ Security awareness training delivered at hire and updated periodically
- ☐ Change management process that triggers security reassessment for material changes