BIZ TECHNOLOGY SOLUTIONS
A New Charter Technologies Company

HIPAA SECURITY COMPLIANCE CHECKLIST

Your Maintaining compliance with the Health Insurance Portability and Accountability Act (HIPAA) is critical for any business handling protected health information (PHI).

This comprehensive checklist is designed to help you navigate and implement the necessary safeguards to protect sensitive data, as outlined in the latest HIPAA compliance rules to meet the required standards, enhancing your cybersecurity posture and ensuring the privacy and security of PHI.

SECURITY EVALUATION

Start here to understand your current cybersecurity posture.

- ☐ Conduct a **Security Evaluation** to assess your organization's tools, policies, and staff readiness.
- ☐ Benchmark results against industry standards and provide executive-level reporting.
- ☐ Use the findings to build a prioritized, actionable roadmap for improvement.

SECURITY AWARENESS AND TRAINING (HIPAA 164.308(A)(5))

Ensure that your workforce is educated, alert, and policy aligned.

- ☐ Conduct mandatory annual HIPAA and cybersecurity training.
- ☐ Train all employees on the proper handling of reproductive health and SUD data, including HIPAA and applicable federal privacy rules such as 42 CFR Part 2.
- ☐ Implement **simulated phishing exercises** to reinforce vigilance and response.

INCIDENT RESPONSE AND RISK MANAGEMENT (HIPAA 164.308(A)(6), 164.308(A)(1))

Demonstrate proactive risk handling and preparedness.

- ☐ Develop and maintain a written incident response plan with defined and documented recovery objectives appropriate to the organization’s risk profile.
- ☐ Conduct and document a comprehensive annual risk analysis covering administrative, physical, and technical safeguards.
- ☐ Review all Business Associate Agreements (BAAs) annually and require 24 hour breach notification clauses.

AUTHENTICATION AND ACCESS CONTROLS (HIPAA 164.312(D), 164.308(A)(3))

Secure access to sensitive systems and data.

- ☐ Enforce strong password policies, including lockout and complexity rules.
- ☐ Require **Multi-Factor Authentication (MFA)** for all remote access, email, and privileged accounts.
- ☐ Apply **Role-Based Access Controls (RBAC)** and regularly audit for inactive or excessive access.

NETWORK AND ENDPOINT PROTECTIONS

Harden systems against internal and external threats.

- ☐ Use a **third-party patch management** solution to keep software up to date.
- ☐ Replace traditional antivirus with **Endpoint Detection and Response (EDR)** tools.
- ☐ Begin planning or documenting progress toward a **Zero Trust architecture**.

FIREWALL AND REMOTE MONITORING (HIPAA 164.312(B), 164.308(A)(1)(I))

Establish robust perimeter defense and oversight.

- ☐ Regularly **review firewall rules** and conduct **penetration testing** to find vulnerabilities.
- ☐ Implement **Intrusion Detection and Prevention Systems (IDS/IPS)**.
- ☐ Use **content filtering** and **VPNs** to secure network access between multiple sites.

ENCRYPTION (HIPAA 164.312(a)(2)(iv))

Ensure data is protected at all stages.

- ☐ Encrypt all laptops, mobile devices, thumb drives, and other removable media.
- ☐ Use **encrypted email** and secure communications tools for transmitting PHI.

BACKUPS (164.308(a)(7)(ii)(A)–(D))

Protect and preserve access to data at all times.

- ☐ Implement **local and encrypted offsite backups**.
- ☐ Include **all PCs and servers** in your backup scope and **test regularly**.
- ☐ Protect backups from **ransomware** and define acceptable downtime (RTO/RPO).
- ☐ Establish a **backup retention policy** and maintain archives for at least **7 years**.

EMAIL SECURITY (HIPAA 164.308(A)(5)(II)(A))

Secure your email environment, a common threat vector.

- ☐ Use **robust spam filtering** and encrypted email solutions.
- ☐ Conduct ongoing **phishing awareness training**.
- ☐ Own and manage your **email domain** to prevent spoofing and ensure legitimacy.

REMOTE ACCESS (HIPAA 164.312(A)(1))

Protect remote connections and access points.

- ☐ Use secure **VPN** or **RDP** for remote work.
- ☐ Employ secure remote tools such as **LogMeIn Pro** or similar platforms.

PASSWORD POLICIES (HIPAA 164.308(A)(5)(II)(D))

Harden credential access organization wide.

- ☐ Enforce **strong, complex password requirements**.
- ☐ Enable **automatic inactivity lockouts** and lockout after failed attempts.

SOFTWARE STANDARDS (HIPAA 164.308(A)(1)(I))

Keep systems current and secure.

- ☐ Ensure that **all operating systems** are supported and regularly updated.
- ☐ Keep **EMR software** up to date and vendor supported.

SYSTEM LIFECYCLE AND DISPOSAL (164.310(d)(2)(i)–(iii))

Avoid data leakage through retired hardware.

- ☐ Replace hardware on a **5-year lifecycle**.
- ☐ Use **DoD-compliant data wiping methods** before disposal of any device with PHI.

LOGGING AND MONITORING (HIPAA 164.312(B))

Track system activity and detect anomalies.

- ☐ Use centralized **log management or SIEM** platforms to monitor activity.
- ☐ Set log **retention policies** and implement routine review procedures.

CLOUD AND SAAS USAGE

Secure and monitor all cloud-based operations.

- ☐ Evaluate the **security posture of cloud vendors** handling PHI.
- ☐ Ensure **data encryption at rest and in transit** within all cloud services.

This framework aligns with HIPAA Security Rule requirements and applicable federal privacy regulations, including 42 CFR Part 2, where applicable. It incorporates both core HIPAA safeguards and recent updates proposed or enforced by the Office for Civil Rights (OCR), a division of the U.S. Department of Health and Human Services (HHS). As a result, this checklist serves as a reliable tool for supporting compliance, strengthening security posture, and preparing organizations for audits or security incidents.