Standards for HIPAA compliance are enforced by HHS Office of Civil Rights,
the Centers for Medicare and Medicaid, and the Federal Trade Commission.

HIPAA
SECURITY RISK CHECKLIST

With the Compliments of

This checklist is designed to help review compliance with the HIPAA Security Rule. It brings together key administrative, physical, technical, and supporting implementation activities that organizations should consider when establishing or improving their security program. Each checklist item identifies a security control or compliance activity, explains the action to be taken, and references the relevant HIPAA Security Rule requirement.

The checklist is intended to be used as a practical working document during HIPAA Security Rule compliance reviews. It is not intended to be completed as a simple pass-or-fail exercise. Organizations should review each item in the context of their own environment, documenting existing controls, identifying any gaps, and recording actions required. This document is intended to complement, rather than replace, a comprehensive HIPAA Security Risk Analysis with a cybersecurity expert.

PLEASE NOTE: This checklist is composed of general questions about the measures your organization should have in place for HIPAA compliance and does not qualify as legal advice. Successfully completing this checklist does not certify that you or your organization are HIPAA compliant.

Section 1: The Incident Response Plan

- [ ] **Core IR Plan Development & Lifecycle Maintenance**

  Action: Draft, approve, and regularly update the master Incident Response Plan, detailing assembly procedures for the Incident Response Team (IRT).

  HIPAA Security Rule: § 164.308(a)(6)(ii) (Response and Reporting).

- [ ] **Plan should include: Workforce Sanction Policy Integration**

  Action: Embed explicit triggers within the containment/investigation phase to loop in HR. If the root-cause analysis determines an internal workforce member intentionally or negligently caused the incident (e.g., data theft, severe policy violation), invoke formal disciplinary actions.

  HIPAA Security Rule: § 164.308(a)(6)(ii) (Response and Reporting).

- [ ] **Plan should include: Post-Incident Risk Assessment & Strategy Update**

  Action: Mandate a "Lessons Learned" phase within the plan. The technical vulnerabilities exposed during the breach must be documented and formally fed back into the enterprise-wide Risk Analysis to update the organization's security posture.

  HIPAA Security Rule: § 164.308(a)(1)(ii)(A) (Risk Analysis).

- [ ] **Plan should include: Breach Notification Rule Cadence & Regulatory Execution**

  Action: Include a dedicated compliance/legal playbook detailing the strict federal timelines. The clock starts at the moment of discovery. The playbook must dictate notification mechanics for affected individuals, HHS/OCR, and local media (if 500 individuals are impacted) within the mandatory 60-day window.

  HIPAA Security Rule: § 164.308(a)(1)(ii)(A) (Risk Analysis).

Section 2: Technical & Evidence Safeguards

- [ ] **Immutable Audit Log Retention**

  Action: Configure system logs, access trails, and network telemetry to ingest into a secure, centralized location (like a dedicated SIEM or write-once-read-many storage). Ensure logs are protected from alteration or deletion by a threat actor attempting to cover their tracks.

  HIPAA Security Rule: § 164.312(b) (Audit Controls).

- [ ] **Pre-Contracted External IR Vendors**

  Action: Establish pre-negotiated Master Service Agreements (MSAs) and active retainers with specialized external breach counsel, cyber forensics firms, and ransomware restoration specialists to bypass procurement delays during a live attack.

  HIPAA Security Rule: § 164.308(a)(6)(ii) (Response and Reporting - managing external dependencies).

Section 3: Business Continuity & Disaster Recovery

- [ ] **Develop a Business Continuity & Disaster Recovery Plan**

  Action: Define clear thresholds for when a security incident requires taking healthcare networks offline. Provide immediate, actionable "paper downtime" workflows for clinicians to continue safe patient care without access to the EHR.

  HIPAA Security Rule: § 164.308(a)(7)(ii)(C) (Emergency Mode Operation Plan).

- [ ] **Plan should include: Applications and Data Criticality Analysis**

  Action: Maintain a prioritized inventory of all software applications, servers, and data repositories containing ePHI. The restoration team must use this predefined tier list to recover clinical systems in order of importance to patient safety.

  HIPAA Security Rule: § 164.308(a)(7)(ii)(E) (Applications and Data Criticality Analysis).

- [ ] **Plan should include: Emergency Access Procedures ("Break-Glass")**

  Action: Establish pre-configured, highly secure alternative authentication pathways. If primary identity management servers (like Active Directory) are encrypted or offline, network administrators must still have a way to gain emergency access to infrastructure.

  HIPAA Security Rule: § 164.312(a)(2)(ii) (Emergency Access Procedure).

Section 4: Testing & Validation

- [ ] **Tabletop Exercises & Simulation Testing**

  Action: Run periodic, scenario-based simulations (e.g., a massive ransomware attack forcing EHR downtime) involving executives, legal, HR, PR, and technical staff to stress-test the linkages between the IR plan, BCDR, and the Breach Notification playbook.

  HIPAA Security Rule: § 164.308(a)(7)(ii)(D) (Contingency Plan Plan Assessment/Testing).