HIPAA Compliance Readiness Checklist

Align with Evolving Security Rule Standards & Strengthen Your Privacy Program

HIPAA is evolving, and enforcement is picking up. Proposed Security Rule updates are shifting from planning to reality – with stricter expectations around MFA, encryption, risk assessments, and vendor oversight.

This checklist helps covered entities and business associates quickly assess their posture, spot compliance gaps, and take action before audits, fines, or breaches occur.

HIPAA SECURITY RULE COMPLIANCE CHECKLIST (2025 EDITION)

1. Technical Safeguards

- ☐ **Multi-Factor Authentication (MFA)** is enabled across all systems accessing ePHI
- ☐ **Encryption** is applied to all ePHI at rest and in transit
- ☐ **Endpoint protection/EDR** is active and up to date
- ☐ **Network segmentation** is enforced to isolate critical systems
- ☐ A documented **patch management process** is operational and timely

💡 *Common Gap: Older backup systems often lack encryption at rest.*

2. Risk Analysis & Vulnerability Management

- ☐ A **comprehensive asset inventory** is maintained and current
- ☐ A **network map** reflects real-time system and data flows
- ☐ **Vulnerability scans** are run at least every 6 months
- ☐ **Penetration testing** is conducted at least once per year
- ☐ Risk assessments include **technical, administrative, and physical safeguards**

3. Incident Response & Internal Policies

- ☐ **Incident response plan (IRP)** is tested and meets 72-hour recovery goal
- ☐ The IRP is **reviewed and updated annually**
- ☐ **Cyber awareness training** is completed annually by all staff
- ☐ **Access controls** are based on least-privilege and actively monitored
- ☐ **Audit logs** and access attempts are reviewed regularly

4. Vendor Management & Business Associate Oversight

- ☐ **Business Associate Agreements (BAAs)** are in place for all vendors and third parties accessing ePHI
- ☐ Vendors submit **annual attestations** of their security practices
- ☐ Vendor access is **regularly reviewed** and risk-tiered
- ☐ A **vendor inventory** is maintained and mapped to critical systems

💡 *Common Gap: Cloud-based tools often fly under the radar of BAA reviews.*

5. Compliance Management & Documentation

- ☐ A **HIPAA gap assessment** reflects the latest rule changes
- ☐ Documentation (IRP, policies, etc.) is **organized and audit-ready**
- ☐ Manual compliance tracking is being replaced with **automated tools**
- ☐ A compliance owner/team is tracking updates and enforcement risks
- ☐ **Audit preparation** is built into your annual review cycle

FAST FACTS*

81% of healthcare leaders say they're ready for HIPAA changes...

45% ...yet only 45% use MFA

and 41% still don't encrypt ePHI at rest or in transit. 41%

Perception ≠ readiness.

**Source: 2025 Healthcare IT Landscape Report*

🚀 WHAT TO DO NEXT

You've identified gaps – now it's time to act.

- Complete a **HIPAA compliance gap assessment** reflecting 2025 rule expectations
- Pilot a **compliance automation platform** to streamline documentation, task tracking, and audits
- Partner with a **healthcare-specialized MSP/MSSP** to implement controls and monitor risk 24x7

💬 NEED SUPPORT?

Let's simplify compliance together. Scan the QR code to schedule a HIPAA readiness assessment with our consulting team.

connect@omegasystemscorp.com
www.omegasystemscorp.com
(610) 678-7002
@omegasystemsMSP

omega systems
technology managed