HIPAA Security Rule Readiness Checklist

A Dean Dorton Insights Resource

This checklist is designed to help healthcare organizations and business associates evaluate readiness for the proposed HIPAA Security Rule updates and strengthen overall cybersecurity and compliance posture.

---

1. Governance & Oversight

☐ Executive leadership is formally engaged in HIPAA security governance
☐ Security and compliance roles and responsibilities are clearly defined
☐ Cybersecurity is included in enterprise risk management and board reporting
☐ Policies and procedures are approved, version-controlled, and reviewed at least annually

---

2. HIPAA Security Risk Analysis

☐ A comprehensive HIPAA Security Risk Analysis has been completed
☐ Risk analysis includes all systems that create, receive, maintain, or transmit ePHI
☐ Threats, vulnerabilities, likelihood, and impact are explicitly documented
☐ Risk analysis is updated regularly and upon material system or operational changes

---

3. Risk Management & Remediation

☐ Identified risks are prioritized and tied to documented remediation plans
☐ Compensating controls are formally documented where full remediation is not feasible
☐ Management approves and tracks risk acceptance decisions
☐ Remediation progress is monitored and reported to leadership

---

4. Technology Asset Inventory & ePHI Mapping

☐ A complete inventory of technology assets touching ePHI is maintained
☐ Inventory includes vendors, cloud services, applications, medical devices, and endpoints
☐ Data flow diagrams identify where ePHI is created, stored, transmitted, and accessed
☐ Asset inventory and data flow documentation are reviewed and updated at least annually

---

5. Technical Safeguards

☐ Encryption is implemented for ePHI at rest and in transit
☐ Multi-factor authentication is enabled for systems accessing ePHI
☐ Access rights are role-based and reviewed periodically
☐ Timely removal of access for terminated or transferred users is enforced
☐ System activity and security event logs are enabled, reviewed, and retained

---

6. Incident Response & Contingency Planning

☐ A written incident response plan exists and is tested periodically
☐ Roles, responsibilities, and escalation paths are clearly defined
☐ Breach notification processes align with HIPAA timelines
☐ Backups are tested and disaster recovery capabilities are documented
☐ Recovery objectives support timely restoration of critical systems and ePHI

---

7. Business Associate Management

☐ Business associates handling ePHI are identified and tracked
☐ Business Associate Agreements (BAAs) are current and comprehensive
☐ Security expectations for vendors are formally defined
☐ Vendor risk assessments or attestations are performed and documented
☐ Subcontractor obligations are addressed where applicable

---

8. Policies, Procedures & Documentation

☐ All HIPAA Security Rule requirements are supported by written documentation
☐ Policies and procedures reflect current systems, risks, and operations

☐ Documentation evidences implementation—not just intent
☐ Records are retained in accordance with regulatory requirements

---

9. Workforce Awareness & Training

☐ HIPAA security awareness training is conducted at least annually
☐ Training addresses phishing, ransomware, and workforce responsibilities
☐ Training completion is tracked and documented
☐ Role-based training is provided where appropriate

---

10. Independent Review & Continuous Improvement

☐ Periodic internal or independent assessments are performed
☐ Findings are tracked through resolution
☐ Lessons learned from incidents and exercises inform program improvements
☐ Compliance posture is reassessed as regulatory expectations evolve

---

How Dean Dorton Can Help

Dean Dorton assists healthcare organizations with HIPAA Security Risk Analyses, readiness assessments, internal audits, and remediation planning aligned to evolving OCR expectations. Our integrated risk, compliance, and cybersecurity approach helps organizations build defensible, scalable security programs—before regulatory changes become enforcement realities.
