HIPAA Security Risk Analysis (SRA) Checklist

A forward-facing, high-level checklist designed to protect patient care, meet OCR expectations, and prepare for Security Rule modernization.

Version: 1.1 | Date: February 12, 2026

Use this checklist as a readiness guide. It is not legal advice and should be tailored to your organization's environment and risk profile.

HIPAA-Aligned Cybersecurity That Protects Patient Care

This checklist is intended for healthcare organizations that want a practical, defensible HIPAA Security Risk Analysis (SRA) and a clear remediation roadmap—without disrupting clinical operations.

Top Risks We See in Healthcare

- "Check-the-box" risk analyses that don't hold up under scrutiny
- Ransomware downtime impacts to clinical operations
- Shared accounts and weak identity controls in clinical settings
- Incomplete backup testing and recovery assumptions

Regulatory Oversight and What's Changing

HIPAA requires covered entities and business associates to conduct an accurate and comprehensive risk analysis of risks to the confidentiality, integrity, and availability of ePHI, and to implement security measures that reduce risk to a reasonable and appropriate level.

OCR has proposed significant updates to the HIPAA Security Rule (NPRM) that, if finalized, would increase specificity and documentation expectations. Regulated entities should begin preparing now by strengthening inventories, evidence, and repeatable governance.

Future-Ready Focus Areas (Based on the NPRM)

- Written documentation for policies, procedures, plans, and analyses, with clearer timelines for compliance
- Technology asset inventory and network map/data flow mapping for where ePHI lives and moves
- More prescriptive, repeatable risk analysis and risk management updates (at least annually and after major changes)
- Stronger expectations for vendor/business associate oversight and verification
- Security control rigor for access control, encryption, monitoring, vulnerability management, and incident response/contingency planning

How to Use This Checklist

- Assess: Mark each item as In Place, Partially In Place, or Not In Place.
- Plan: Convert gaps into a prioritized remediation roadmap (people, process, technology).
- Build: Implement controls with minimal disruption to clinical workflows.
- Maintain: Re-validate at least annually and after major environment changes or security incidents.

Scope and Inputs

Before starting, confirm the scope of ePHI and the systems that create, receive, maintain, or transmit ePHI (and systems that can affect ePHI).

Pre-Work Inputs

- Business context: locations, services, clinical workflows, and downtime tolerances
- Technology asset inventory (endpoints, servers, cloud services, network equipment, medical/IoT devices, applications)
- Identity sources (EHR, IAM/SSO, privileged accounts, shared accounts, contractors)
- Third parties and business associates (BAAs, integrations, managed services, cloud hosting, EHR vendors)
- Existing policies, incident response plan, disaster recovery plan, backup procedures, and prior assessments

SRA Method (Aligned to OCR Risk Analysis Guidance)

1. Identify where ePHI is created, received, maintained, or transmitted (systems, apps, devices, storage, integrations).

2. Identify and document reasonably anticipated threats (e.g., ransomware, credential theft, insider misuse, lost devices).

3. Identify vulnerabilities and predisposing conditions (e.g., weak MFA, unpatched systems, flat networks, shared accounts).

4. Assess current security measures and whether controls are configured and used effectively.

5. Determine likelihood of threat occurrence for each threat/vulnerability pair.

6. Determine potential impact (patient care disruption, data confidentiality/integrity loss, financial/legal exposure).

7. Determine level of risk and document corrective actions to reduce risk to a reasonable and appropriate level.

8. Finalize documentation and integrate results into an ongoing risk management program (revisit after major changes).

Administrative Safeguards Checklist

Checklist item	What good looks like	Status / notes
☐ Security leadership designated (Security Officer + backups)	Named roles with authority; responsibilities documented; regular reporting cadence.	In Place / Partial / Not In Place
☐ Policies and procedures are written, current, and approved	Policies cover Security Rule safeguards, access control, IR, backup/DR; reviewed at least annually.	In Place / Partial / Not In Place
☐ Technology asset inventory is complete and maintained	Hardware/software/service inventory includes owner, version, location; updated on change + at least annually.	In Place / Partial / Not In Place

Checklist item	What good looks like	Status / notes
☐ Network map and ePHI data flow mapping maintained	Data flows show where ePHI enters/exits systems and how it is accessed remotely/externally; supports segmentation decisions.	In Place / Partial / Not In Place
☐ Risk analysis is documented and repeatable	Written SRA that covers all ePHI and supporting systems; includes likelihood/impact and rationale.	In Place / Partial / Not In Place
☐ Risk management program with tracked remediation	Risk register and remediation roadmap with owners, due dates, evidence, and executive sign-off.	In Place / Partial / Not In Place
☐ Workforce security + role-based access governance	Access based on role; onboarding/offboarding SLAs; periodic access reviews; shared accounts eliminated or tightly controlled.	In Place / Partial / Not In Place
☐ Security awareness training and phishing resilience	Initial + annual training; role-based training for admins; phishing testing; exception handling documented.	In Place / Partial / Not In Place
☐ Vendor / business associate oversight	Inventory of vendors with ePHI exposure; BAAs in place; security due diligence and ongoing monitoring documented.	In Place / Partial / Not In Place
☐ Incident response plan supports ransomware and clinical downtime	IR plan includes decision-making, comms, containment, downtime workflows, and tabletop exercises.	In Place / Partial / Not In Place
☐ Contingency planning, backups, and recovery testing	Backups are immutable/offline where feasible; tested restores; defined RTO/RPO; DR plan exercised.	In Place / Partial / Not In Place
☐ Ongoing evaluation after major changes	Formal review when systems change, new threats emerge, M&A occurs, or incidents happen; SRA updated accordingly.	In Place / Partial / Not In Place

Physical Safeguards Checklist

Checklist item	What good looks like	Status / notes
☐ Facility access controls for areas housing systems with ePHI	Badge/visitor controls; server rooms secured; logs maintained; procedures for emergencies.	In Place / Partial / Not In Place
☐ Workstation and clinical device controls	Screen-lock policies; privacy screens where needed; kiosk/shared workstation controls; automatic logoff in clinical areas.	In Place / Partial / Not In Place

Checklist item	What good looks like	Status / notes
☐ Device and media controls (mobile, laptops, removable media)	Inventory; encryption; secure disposal; lost device process; restrictions on removable media.	In Place / Partial / Not In Place
☐ Remote work / home office safeguards	Managed endpoint controls; secure Wi-Fi guidance; VPN/zero-trust access; MDM for mobile where applicable.	In Place / Partial / Not In Place
☐ Medical/IoT devices risk-managed	Medical device inventory; network segmentation; vendor patching/compensating controls; monitoring.	In Place / Partial / Not In Place

Technical Safeguards Checklist

Checklist item	What good looks like	Status / notes
☐ Unique user identification and strong authentication	No shared logins for ePHI access; MFA for remote, privileged, and high-risk access; break-glass documented.	In Place / Partial / Not In Place
☐ Access control and least privilege	Role-based access; privileged access management where feasible; periodic access reviews; rapid termination.	In Place / Partial / Not In Place
☐ Audit controls and centralized logging	Logs for EHR, identity, endpoints, servers, network; alerting for suspicious activity; retention aligned to policy.	In Place / Partial / Not In Place
☐ Malware protection and endpoint detection/response	Modern EDR; anti-malware; application control where feasible; isolation/containment playbooks.	In Place / Partial / Not In Place
☐ Vulnerability management and patching	Regular scanning; prioritized patching; remediation SLAs; exception process; legacy systems isolated.	In Place / Partial / Not In Place
☐ Integrity controls for critical systems/data	File integrity monitoring where appropriate; secure configurations; change control; backups validated.	In Place / Partial / Not In Place
☐ Encryption in transit	TLS for web/EHR integrations; secure email options; VPN/secure tunnels; secure remote admin (no plaintext protocols).	In Place / Partial / Not In Place
☐ Encryption at rest and key management	Device/server/storage encryption; managed keys; access to keys restricted; documented exceptions/compensating controls.	In Place / Partial / Not In Place

Checklist item	What good looks like	Status / notes
☐ Network segmentation and secure connectivity	ePHI systems segmented from guest/admin networks; least-privilege network paths; remote access controlled.	In Place / Partial / Not In Place
☐ Backup protection against ransomware	Immutable backups; separate credentials; backup monitoring; restore tests; offline copies where feasible.	In Place / Partial / Not In Place

Ransomware + Clinical Downtime Readiness

- Downtime procedures for EHR outages and clinical operations are documented and practiced
- Decision tree for isolate vs. power down vs. maintain connectivity (patient safety first)
- Rapid containment capabilities (EDR isolation, account disablement, network blocks) are tested
- Backups and restores validated for critical systems; recovery sequencing defined
- Tabletop exercise schedule includes ransomware and downtime scenarios

Evidence Pack (What OCR Expects to See)

- Written SRA report (scope, methodology, findings, risk ratings, corrective actions)
- Technology asset inventory and ePHI data flow / network map
- Risk register and remediation tracking with evidence of completion
- Policies/procedures (access, IR, backup/DR, vulnerability management, training) with review dates
- Training records and security awareness metrics
- Vendor/BAA inventory and due diligence documentation
- Backup restore test results and tabletop exercise after-action reports
- Logs or monitoring evidence demonstrating detection/response capability

How STIG Helps

STIG helps healthcare organizations reduce cyber risk without disrupting patient care—through HIPAA Security Risk Analysis (SRA), ransomware readiness, and 24×7 security operations built on CrowdStrike with automation.

HEALTHCARE

What We Deliver

- HIPAA SRA + remediation roadmap
- CrowdStrike-native security operations (MDR) with Torq automation
- Healthcare pen testing (external/web/validation)
- Ransomware + downtime IR tabletop exercises
- Security awareness + managed phishing (KnowBe4)

References

- HHS OCR - HIPAA Security Rule NPRM factsheet (HHS.gov)
- Federal Register - HIPAA Security Rule NPRM (Jan 6, 2025)
- HHS OCR - Guidance on Risk Analysis (HHS.gov)
- HHS - Healthcare and Public Health (HPH) Cybersecurity Performance Goals (HHS Cyber Gateway)