FREE RESOURCE

TECHCURO

HIPAA AI Risk Self-Assessment Checklist

A 30-minute assessment for healthcare practices that are already using AI tools or getting ready to. Score yourself, find the gaps, and walk away with a clear remediation path.

> **How to use this checklist:** Work through each section with your IT lead or office manager. Check every item that is currently satisfied. Tally your score at the end. Items marked HIGH risk require immediate attention before expanding AI use.

1 AI Vendor Inventory

45 CFR 164.308(a)(1)

- ☐ We have a **written list of every AI tool** staff currently uses (including personal accounts like ChatGPT free, Gemini, etc.) — HIGH
- ☐ Each tool is classified as **PHI-touching or non-PHI** based on what data flows through it — HIGH
- ☐ We have confirmed which vendors will **sign a Business Associate Agreement (BAA)** — HIGH
- ☐ Consumer-grade AI tools (ChatGPT free, Gemini free, Perplexity) are **blocked or banned by policy** for work use — HIGH
- ☐ We review the vendor list at least **annually** or when a new AI tool is adopted — MED

2 Business Associate Agreements (BAAs)

45 CFR 164.314(a)(1)

- [ ] Signed BAAs exist for **all AI vendors** that process, store, or transmit PHI — HIGH
- [ ] Each BAA covers the **specific AI product/tier** in use (e.g., OpenAI Enterprise ≠ OpenAI free tier) — HIGH
- [ ] BAAs are stored in a **central, accessible location** and reviewed by counsel — MED
- [ ] BAA **renewal dates are tracked** and reviewed before expiry — MED
- [ ] Vendor subprocessor lists are reviewed and we know who the vendor's **sub-BAAs cover** — MED

3 Data Flow & PHI Exposure

45 CFR 164.308(a)(1), 164.312(c)

- [ ] We have a **data flow diagram** showing where PHI enters and exits AI systems — HIGH
- [ ] Staff are trained **not to paste PHI** into general-purpose AI prompts — HIGH
- [ ] Clinical scribe or documentation AI uses **Zero Data Retention (ZDR)** or equivalent control — HIGH
- [ ] EHR data exports fed to AI are **de-identified or encrypted** in transit — HIGH
- [ ] AI-generated outputs containing PHI are **stored under the same controls** as other PHI records — MED
- [ ] We have confirmed **AI model training opt-out** for all PHI-touching vendors — MED

4 Access Controls & Endpoint Security

45 CFR 164.312(a)(1), 164.312(a)(2)(i)

- [ ] Access to PHI-touching AI tools is **role-based and logged** — HIGH
- [ ] Shared logins or shared API keys for AI tools are **not in use** — HIGH
- [ ] MFA is enabled on all AI platform accounts that touch PHI — MED
- [ ] Offboarding procedure includes **revoking AI tool access** within 24 hours of staff departure — MED
- [ ] Devices used to access AI tools are **enrolled in MDM** or meet minimum security baseline — LOW

5 Audit Logging & Incident Response

45 CFR 164.312(b), 164.308(a)(6)

- [ ] AI vendor audit logs are **accessible to us** (not just retained by the vendor) — HIGH
- [ ] We have a **documented incident response plan** that includes AI-related PHI exposure scenarios — HIGH
- [ ] Logs are retained for **at least 6 years** per HIPAA requirement — MED
- [ ] We have tested our incident response with a **tabletop exercise** in the last 12 months — LOW

6 Workforce Training & Policy

45 CFR 164.308(a)(5), 164.316(a)

- [ ] There is a **written AI Acceptable Use Policy** specific to your practice — HIGH
- [ ] All staff have **signed and acknowledged** the AI use policy — MED
- [ ] Annual HIPAA training covers **AI-specific scenarios** (prompt injection, data leakage, vendor risk) — MED
- [ ] A designated person is responsible for **AI compliance oversight** (Privacy/Security Officer or equivalent) — MED
- [ ] Policy is **reviewed and updated annually** or when new AI tools are adopted — LOW

Your Score

CHECKED	HIGH RISK GAPS	READY FOR AI?
__ / 30	__	___ %
items satisfied	unchecked HIGH items	checked ÷ 30 × 100

25 to 30	Strong Foundation	Well-controlled. Focus on continuous monitoring and annual reviews.
18 to 24	Moderate Risk	Targeted remediation needed. Prioritize all unchecked HIGH items immediately.
10 to 17	Significant Exposure	Do not expand AI use until HIGH-risk gaps are closed. OCR audit liability is real.
0 to 9	Critical Risk	Pause PHI-touching AI use. Immediate assessment and remediation required.

This checklist is an educational tool, not legal advice. It does not constitute a formal HIPAA risk analysis under 45 CFR 164.308(a)(1). Consult qualified counsel for compliance determinations.