



ReasonNotes

FREE CLINICAL RESOURCE

HIPAA Compliance Checklist for AI Tools

Questions to ask and boxes to check before you use AI with patient information.

Free to use and share in your practice.

Want notes written for you? Try ReasonNotes free at reasonnotes.com

A Practical Guide for Practice Administrators

TABLE OF CONTENTS

1. Understanding HIPAA as It Applies to AI Tools
2. Penalty Tiers and Real Enforcement Cases
3. Business Associate Agreement (BAA) Requirements
4. Technical Safeguard Requirements
5. Questions to Ask AI Vendors Before Signing
6. Compliance Checklist Summary
7. Key Regulatory References

SECTION 1: UNDERSTANDING HIPAA AS IT APPLIES TO AI TOOLS

Any AI tool that creates, receives, maintains, or transmits electronic protected health information (ePHI) on behalf of a covered entity is subject to HIPAA. This includes:

- AI-powered clinical note generation and medical scribes
- AI diagnostic tools analyzing patient imaging, labs, or records
- NLP tools processing clinical transcripts
- AI chatbots interacting with patients about health conditions
- Voice recognition and transcription services
- AI-based clinical decision support systems

KEY REGULATORY DEVELOPMENTS (2025)

On January 6, 2025, HHS OCR proposed the first major update to the HIPAA Security Rule in 20 years. Key changes include:

- **ELIMINATION** of the distinction between "required" and "addressable" implementation specifications. ALL safeguards become mandatory.
- **MANDATORY** multi-factor authentication (MFA) for all systems accessing ePHI.
- **MANDATORY** vulnerability scanning at least every six months.
- **MANDATORY** penetration testing at least annually.
- **MANDATORY** patch management: critical patches within 15 days, high-risk patches within 30 days.
- **MANDATORY** 24-hour notification from business associates to covered entities upon activation of contingency plans.

On January 10, 2025, OCR issued a "Dear Colleagues" letter confirming it will enforce Section 1557 nondiscrimination protections as applied to AI use in healthcare (effective May 1, 2025).

SECTION 2: PENALTY TIERS AND REAL ENFORCEMENT CASES

CURRENT HIPAA CIVIL PENALTY TIERS (2025-2026, inflation-adjusted):

Tier 1 - Did Not Know: \$145 - \$73,011 per violation Tier 2 - Reasonable Cause: \$1,461 - \$73,011 per violation Tier 3 - Willful Neglect,

Corrected: \$14,602 - \$73,011 per violation

Tier 4 - Willful Neglect,

NOT Corrected: \$73,011 - \$2,190,294 per violation

Annual Cap: \$2,190,294 per tier

Criminal penalties: up to \$250,000 and 10 years imprisonment.

REAL ENFORCEMENT CASES INVOLVING TECHNOLOGY

Blackbaud, Inc. (2023-2024)

- Ransomware attack on cloud computing vendor serving healthcare
- Fine: \$49.5 million multistate + \$6.75 million California settlement

Advocate Aurora Health (2024)

- Meta Pixel tracking code transmitted PHI to Facebook without consent
- Fine: \$12.25 million settlement; 3 million patients affected

Mass General Brigham (2024)

- Cookies and analytics tools shared patient data with third parties
- Fine: \$18.4 million class action settlement

BetterHelp (2023)

- Telehealth platform shared mental health data via tracking technologies
- Fine: \$7.8 million FTC settlement

GoodRx (2023)

- Health app exposed prescription data through third-party trackers
- Fine: \$25 million class action settlement

Montefiore Medical Center (2024)

- Employee stole and sold patient data; inadequate access controls
- Fine: \$4.75 million; 12,517 individuals affected

TOTAL from tracking technology violations alone: Over \$100 million in combined penalties 2023-2025. OCR wrote to nearly 130 healthcare organizations in July 2023 warning about tracking technology risks.

SECTION 3: BUSINESS ASSOCIATE AGREEMENT (BAA) REQUIREMENTS

Any AI vendor handling PHI is a Business Associate. A BAA is LEGALLY REQUIRED before any PHI is shared.

Regulatory basis: 45 CFR 164.314(a), 45 CFR 164.504(e), 45 CFR 164.308(b)(1)

MANDATORY BAA PROVISIONS

- ☐ Permitted and Required Uses/Disclosures
- ☐ Safeguard Requirements (BA must comply with Security Rule)
- ☐ Subcontractor Requirements (all sub-BAs must also have BAAs)
- ☐ Breach Notification (current: 60 days; proposed: 24 hours)
- ☐ Individual Rights Support (access, amendment, accounting)
- ☐ HHS Access (BA must allow HHS compliance reviews)
- ☐ Return or Destruction of PHI upon termination
- ☐ Term and Termination provisions

AI-SPECIFIC BAA PROVISIONS YOU SHOULD ADD

- ☐ PHI must NOT be used for model training without authorization
- ☐ PHI must NOT be aggregated with other customers' data
- ☐ PHI must NOT be retained beyond the service period
- ☐ Specify data residency (geographic restrictions)
- ☐ Right to inspect vendor's security practices
- ☐ AI-specific incident response (hallucinations, model errors)
- ☐ Subcontractor chain fully documented (cloud providers, APIs)

VENDORS CURRENTLY OFFERING BAAs FOR AI SERVICES:

- OpenAI (API/Enterprise - must be requested)
- Microsoft Azure (Azure OpenAI Service)
- Google Cloud (Vertex AI)
- Amazon Web Services (Amazon Bedrock)

WARNING: A vendor offering a BAA does NOT mean they are HIPAA compliant. The BAA is a legal agreement, not a certification. Due diligence required.

SECTION 4: TECHNICAL SAFEGUARD REQUIREMENTS

Per 45 CFR 164.312 and proposed 2025 Security Rule updates:

ENCRYPTION

- ☐ Data at Rest: AES-256 encryption minimum
- ☐ Data in Transit: TLS 1.2 or TLS 1.3 (TLS 1.0/1.1 unacceptable)

- ☐ Perfect Forward Secrecy (PFS) enabled
- ☐ Key management and rotation policies documented

SAFE HARBOR: If ePHI is encrypted per NIST standards and a breach occurs, breach notification may not apply (NIST SP 800-111, 800-52).

ACCESS CONTROLS

- ☐ Unique User Identification - no shared accounts (164.312(a)(2)(i))
- ☐ Multi-Factor Authentication for all users (proposed 2025 rule)
- ☐ Role-Based Access Control with least privilege
- ☐ Automatic Logoff after inactivity (164.312(a)(2)(iii))
- ☐ Emergency Access Procedures documented (164.312(a)(2)(ii))

AUDIT CONTROLS

- ☐ Log who accessed data, when, what, and actions taken
- ☐ Logs tamper-resistant and retained per policy
- ☐ Regular review of audit logs
- ☐ For AI: log all queries containing PHI and all AI outputs with PHI

VULNERABILITY MANAGEMENT (Proposed 2025 Rule):

- ☐ Vulnerability scanning every 6 months minimum
- ☐ Penetration testing annually minimum
- ☐ Critical patches deployed within 15 days
- ☐ High-risk patches deployed within 30 days

SECTION 5: QUESTIONS TO ASK AI VENDORS BEFORE SIGNING

DATA HANDLING

1. Exactly what PHI will your system access, process, and store?
2. Where is PHI stored geographically? Any data outside the US?
3. How is PHI encrypted at rest and in transit? Specific algorithms?
4. Do you use PHI to train or improve your AI models?
5. What happens to our PHI if we terminate the contract?
6. What is your data retention policy?

SECURITY AND COMPLIANCE

7. Will you sign a BAA?
8. Do you have a current SOC 2 Type II report or HITRUST certification?
9. When was your last independent security audit and penetration test?
10. Do you support MFA for all users?
11. What is your patch management process and timeline?

12. Do you have a dedicated security team?

INCIDENT RESPONSE

13. What is your breach notification timeline?

14. Do you have a documented incident response plan? Last tested?

15. What was the last security incident you experienced?

16. Do you carry cyber liability insurance? Coverage limits?

AI-SPECIFIC

17. How do you prevent AI hallucinations generating false patient info?

18. What safeguards prevent the AI from memorizing patient data?

19. How do you validate AI outputs for clinical accuracy?

20. What is your process for AI bias/discrimination? (Section 1557)

21. Can you provide audit logs of all AI interactions involving our PHI?

22. If you use third-party AI models (OpenAI, Anthropic, Google), do you have BAAs with those providers?

SUBCONTRACTORS

23. What cloud provider(s) do you use? (AWS, Azure, GCP?)

24. Do you have BAAs with all infrastructure providers?

25. What other subcontractors have access to our PHI?

RED FLAGS - WALK AWAY IF

- Vendor refuses to sign a BAA
- Cannot produce a recent independent security audit
- Uses PHI for model training without clear de-identification
- Cannot explain encryption standards
- Stores PHI outside the US without disclosure
- Has no documented incident response plan
- Cannot identify subcontractors that access PHI

SECTION 6: COMPLIANCE CHECKLIST SUMMARY

BEFORE ADOPTING ANY AI TOOL

- ☐ Determine if tool creates, receives, maintains, or transmits ePHI
- ☐ Conduct vendor due diligence
- ☐ Execute BAA with all required provisions
- ☐ Update organization's risk analysis to include the new AI tool
- ☐ Document evaluation and decision-making process

TECHNICAL REQUIREMENTS

- ☐ AES-256 encryption at rest
- ☐ TLS 1.2+ encryption in transit with PFS

- ☐ Multi-factor authentication for all users
- ☐ Unique user identification (no shared accounts)
- ☐ Role-based access control with least privilege
- ☐ Automatic session logoff
- ☐ Comprehensive audit logging
- ☐ Vulnerability scanning every 6 months
- ☐ Penetration testing annually
- ☐ Critical patches within 15 days

ADMINISTRATIVE REQUIREMENTS

- ☐ Designated security officer for AI tool compliance
- ☐ Written policies for AI tool use with PHI
- ☐ Workforce training on AI tool use and PHI handling
- ☐ Incident response plan covering AI-specific scenarios
- ☐ Regular risk assessments (at least annually)

PRIVACY REQUIREMENTS

- ☐ Minimum necessary standard applied (45 CFR 164.502(b))
- ☐ Notice of Privacy Practices updated to reflect AI use
- ☐ Patient right of access preserved for AI-generated records
- ☐ Accounting of disclosures includes AI vendor disclosures

AI-SPECIFIC REQUIREMENTS

- ☐ PHI not used for model training without authorization
- ☐ De-identification verified per Safe Harbor or Expert Determination
- ☐ AI bias and discrimination risk assessed (Section 1557)
- ☐ AI-generated content distinguished from source clinical data
- ☐ Subcontractor chain fully documented with BAAs at every level
- ☐ Data deletion/return procedures defined for contract termination

SECTION 7: KEY REGULATORY REFERENCES

HIPAA Privacy Rule:

45 CFR 164.502 Uses and disclosures 45 CFR 164.504(e) BAA requirements 45 CFR 164.514
De-identification standards 45 CFR 164.524 Individual right of access 45 CFR 164.530(j)
Documentation retention (6 years)

HIPAA Security Rule:

45 CFR 164.308 Administrative safeguards 45 CFR 164.310 Physical safeguards 45 CFR
164.312 Technical safeguards 45 CFR 164.314 Organizational requirements (BAA standards)

Breach Notification Rule:

45 CFR 164.404 Notification to individuals (60 days) 45 CFR 164.410 BA notification to covered entity

Other:

HITECH Act, Section 13401 - Security provisions for BAs Section 1557 of the ACA -
Nondiscrimination, including AI NIST SP 800-111 - Storage Encryption Technologies NIST
SP 800-52 - TLS Implementation Guidelines

DISCLAIMER: This guide is for informational purposes only and does not constitute legal advice.
Consult qualified legal counsel for advice tailored to your organization's specific circumstances.

Prepared by ReasonNotes | reasonnotes.com