

HIPAA Audit Prep Checklist

For digital health and health-adjacent software companies that handle protected health information (PHI) for US healthcare customers. It follows the HIPAA Security Rule safeguards, adds the Breach Notification Rule and business associate duties, and says what evidence a customer, auditor or investigator will ask to see.

Updated September 2026. A starting point, not legal advice. Your obligations depend on your contracts and on whether you are a covered entity or a business associate.

Before you start

- There is no HIPAA certification.** Nobody can certify you "HIPAA compliant". What buyers accept is evidence: a current risk analysis, policies, a signed business associate agreement (BAA), and often an independent assessment such as a SOC 2 with HIPAA mapping or a HITRUST certification.
- You are probably a business associate.** If you create, receive, keep or transmit PHI on behalf of a covered entity (a provider, health plan or clearinghouse), you are directly liable under the Security Rule and for breach notification to your customer.
- The risk analysis is the foundation.** 45 CFR 164.308(a)(1) requires an accurate and thorough risk analysis. Its absence is one of the findings the HHS Office for Civil Rights (OCR) cites most often in enforcement, and OCR has run a dedicated initiative on it.
- Check for rule changes.** HHS proposed significant updates to the Security Rule in January 2025, including making more safeguards mandatory. Confirm the current status before you finalise policies.

Typical timeline for a small company

Step	Typical duration
Map where PHI lives and flows	1 to 2 weeks
Risk analysis and risk management plan	2 to 4 weeks
Policies, BAAs and missing safeguards	4 to 10 weeks
Training, testing and evidence in place	2 to 4 weeks

1. Administrative safeguards (45 CFR 164.308)

☐ **A documented risk analysis covering every system that touches ePHI**

It must identify where ePHI is, the threats to it, current controls, likelihood, impact and resulting risk. A generic template filled in once does not meet "accurate and thorough".

Evidence: the analysis with its date, scope, method and results; the ePHI inventory it was based on.

☐ **A risk management plan that reduces the risks you found**

Evidence: a plan with owners and dates, and progress records.

☐ **A named security official**

One person responsible for developing and implementing the security policies. A privacy official is also required of covered entities; business associates often name one anyway.

Evidence: a written designation.

☐ **Workforce security and access management**

Only people who need ePHI get access, access is authorised, and it ends when employment ends.

Evidence: access request and approval records; termination checklists; periodic access reviews.

☐ **Security awareness training, with periodic reminders**

Evidence: completion records by person and date; phishing or reminder campaigns.

☐ **A sanction policy applied to staff who violate policy**

Evidence: the policy and, where relevant, records of its use.

☐ **Information system activity review**

Someone regularly reviews audit logs, access reports and security incident tracking.

Evidence: a review schedule and dated review records.

☐ **Security incident procedures**

Evidence: an incident response plan and an incident log.

☐ **A contingency plan: backup, disaster recovery and emergency mode operation**

Evidence: backup configuration, a tested restore, a DR plan with recovery objectives.

☐ **A periodic evaluation of your safeguards**

Evidence: an annual technical and non-technical evaluation, such as an internal review or external assessment.

☐ **Business associate agreements with every subcontractor that handles ePHI**

Your cloud host, email provider, support tool and analytics vendor may all need one. No BAA means that vendor should not see PHI.

Evidence: a vendor list showing which touch PHI, and signed BAAs for each.

2. Physical safeguards (164.310)

☐ **Facility access controls, or reliance on your cloud provider documented**

Evidence: office access controls if PHI is accessed there; your cloud provider's assurance reports.

☐ **Workstation use and security rules**

Evidence: a policy; MDM showing disk encryption, screen lock and patching.

☐ **Device and media disposal and reuse**

Evidence: wiping or destruction records.

3. Technical safeguards (164.312)

☐ **Unique user IDs, emergency access and automatic logoff**

Evidence: identity provider settings; session timeout configuration; a documented break-glass procedure.

☐ **Encryption of ePHI at rest and in transit**

"Addressable" in the current rule, which means you must implement it or document why an alternative is reasonable. In practice buyers expect encryption, and encrypted data that is lost can fall outside breach notification.

Evidence: storage, database and backup encryption settings; TLS configuration.

☐ **Audit controls that record activity in systems holding ePHI**

Evidence: application and infrastructure logs showing who accessed what, with retention.

☐ **Integrity controls and person or entity authentication**

Evidence: MFA settings; checksums or database controls that protect records from improper change.

4. Organisational and documentation requirements (164.314, 164.316)

☐ **Policies and procedures written down and available to staff**

Evidence: the policy set with approval dates.

☐ **Documentation kept for six years**

HIPAA requires policies, risk analyses and related records to be kept for six years from creation or last effective date.

Evidence: a retention setting or archive with older versions.

5. Breach notification (164.400 to 164.414)

☐ **A procedure to assess whether an incident is a reportable breach**

Unsecured PHI that is acquired, accessed, used or disclosed improperly is presumed a breach unless a documented four-factor risk assessment shows a low probability of compromise.

Evidence: the procedure and completed assessments.

☐ **Customer notification timelines match your BAA**

A business associate must notify the covered entity without unreasonable delay and no later than 60 days after discovery. Many BAAs set a shorter period, so check each one.

Evidence: a table of customers and their contractual notification periods.

Common mistakes

- A risk analysis that lists controls but never identifies where ePHI actually lives.
- PHI in tools without a BAA: support tickets, error logs, analytics, email.
- Test and staging environments loaded with real patient data.
- Assuming the cloud provider's BAA covers your application. It covers their services, configured correctly by you.
- No record of the annual evaluation, so the program looks frozen in time.

Canadian notes

- A Canadian company serving US covered entities is bound by HIPAA through its BAAs, and also by Canadian privacy law for the data it holds.
- If you also handle Canadian health information, provincial health privacy laws apply, such as PHIPA in Ontario, with their own breach reporting duties. PIPEDA applies to commercial activity where no substantially similar provincial law does.
- Data residency: some Canadian public health customers require data to stay in Canada. Check before you choose regions or subprocessors.

What to do next

1. Draw where PHI enters, where it is stored, and every system and vendor it touches.

2. Run the risk analysis against that map, not against a generic list.
3. Get BAAs in place, or remove PHI from any tool that cannot sign one.
4. Close encryption, access and logging gaps first. They are what customers test.
5. Decide what independent evidence your buyers want (SOC 2 with HIPAA mapping, HITRUST, or an assessment letter) and plan for it.

Want a second pair of eyes? TrazTech runs security and compliance readiness as fixed-scope work for software companies. Book a free 30-minute readiness call at traztech.ca/free-readiness-call, or get The Compliance Brief, one short email every Tuesday, at traztech.ca/brief.

© 2026 TrazTech Inc. · traztech.ca · Prepared by Jacob Masse, Principal. A starting point, not legal or audit advice.