

HIPAA-for-AI

If your AI system can see, store, or infer Protected Health Information, HIPAA is not optional. This pack focuses on the Security Rule controls that have a clean evidence story in Beacon — receipts, signing, access logs, BAAs, and minimum necessary use.

AUTHORITY	U.S. Department of Health and Human Services (HHS / OCR)
PUBLICATION	45 CFR Parts 160, 162, 164
VERSION	1.0.0 · License: Apache-2.0
URL	https://www.hhs.gov/hipaa/index.html

About this pack

This is the HIPAA-for-AI pack from the AIGovOps Beacon audit framework. Walk it with your auditor, your CISO, and the engineer who actually ships the system. It is short on purpose.

Items marked **auto** are computed by Beacon from signed receipts and the model inventory — you do not have to hand-evidence them, the platform does. Items without that badge require a human attestation: a person reads the prompt, checks the evidence is real, and ticks a box. Beacon records the attestation as a signed receipt with `event_type attestation`.

The severity label tells you how much weight an item carries in the production-readiness gate. Critical items can fail a release on their own. Lower-severity items contribute to a weighted score.

This pack is released under the Apache License 2.0. The underlying source publication retains its own copyright; consult it for normative language.

Checklist — Functions

ADMIN

Administrative safeguards

45 CFR § 164.308 — administrative actions, policies, and procedures.

ADMIN-1.1

CRITICAL

Has a Security Risk Analysis been performed that explicitly includes the AI system?

Evidence `sra_uri` Gate `sra_includes_ai`

☐ Yes ☐ No ☐ N/A

ADMIN-1.2

HIGH

Is a designated Security Official accountable for the AI system?

Evidence `security_official_named`

☐ Yes ☐ No ☐ N/A

ADMIN-1.3

HIGH

Are workforce members granted access on a need-to-know basis with documented authorization?

Evidence access_authorization_log

☐ Yes ☐ No ☐ N/A

ADMIN-1.4

MEDIUM

Is workforce training on AI-specific PHI handling delivered and recorded?

Evidence training_log_uri

☐ Yes ☐ No ☐ N/A

ADMIN-1.5

MEDIUM

Are sanctions for workforce members who fail to comply documented and applied?

Evidence sanctions_policy_uri

☐ Yes ☐ No ☐ N/A

ADMIN-1.6

HIGH

Is there a contingency plan covering AI system failure, including data backup and disaster recovery?

Evidence contingency_plan_uri

☐ Yes ☐ No ☐ N/A

BAA

Business associate agreements

45 CFR § 164.502(e) and § 164.504(e).

BAA-2.1

CRITICAL

AUTO

Is a Business Associate Agreement in place for every AI vendor that processes PHI?

Evidence baa_uri Gate baa_for_each_phi_vendor

☐ Yes ☐ No ☐ N/A

BAA-2.2

CRITICAL

Do BAAs explicitly address training-data use, retention, and subprocessor disclosure?

Evidence baa_review_signoff

☐ Yes ☐ No ☐ N/A

BAA-2.3

MEDIUM

Are vendor security attestations (HITRUST, SOC 2 Type II) collected and current?

Evidence vendor_attestation_uri

☐ Yes ☐ No ☐ N/A

PHYS

Physical safeguards

45 CFR § 164.310. Most relevant when Beacon runs on-prem.

PHYS-3.1

MEDIUM

Are facility access controls in place where AI systems process PHI?

Evidence facility_access_policy

☐ Yes ☐ No ☐ N/A

PHYS-3.2

MEDIUM

Are workstation use policies enforced for endpoints that can prompt PHI-touching models?

Evidence workstation_policy_uri

☐ Yes ☐ No ☐ N/A

TECH

Technical safeguards

45 CFR § 164.312.

TECH-4.1

CRITICAL

AUTO

Is unique user identification enforced for all AI system access (OIDC-bound, no shared accounts)?

Evidence beacon_user_subject_present Gate unique_user_id

☐ Yes ☐ No ☐ N/A

TECH-4.2

MEDIUM

Is automatic logoff implemented for AI interfaces?

Evidence idle_timeout_config

☐ Yes ☐ No ☐ N/A

TECH-4.3

CRITICAL

Is PHI encrypted at rest where stored or cached by the AI system?

Evidence encryption_at_rest_attestation

☐ Yes ☐ No ☐ N/A

TECH-4.4

CRITICAL

Is PHI encrypted in transit between caller, gateway, and model provider?

Evidence `tls_attestation`

☐ Yes ☐ No ☐ N/A

TECH-4.5

CRITICAL

AUTO

Are AI invocations logged with audit controls sufficient to reconstruct who, what, when?

Evidence `beacon_receipts_active` `Gate receipts_captured`

☐ Yes ☐ No ☐ N/A

TECH-4.6

CRITICAL

AUTO

Are receipts protected against alteration (cryptographic signature, append-only storage)?

Evidence `beacon_signature_verify` `Gate signatures_valid`

☐ Yes ☐ No ☐ N/A

TECH-4.7

HIGH

Is the minimum-necessary principle enforced in prompts and results (PHI redaction, scope-of-use checks)?

Evidence `redaction_policy_uri` `Gate redaction_enabled`

☐ Yes ☐ No ☐ N/A

BREACH

Breach notification

45 CFR §§ 164.400 – 164.414.

BREACH-5.1

CRITICAL

Is there a documented process to assess and report AI- involved PHI incidents within HIPAA timelines?

Evidence `breach_runbook_uri`

☐ Yes ☐ No ☐ N/A

BREACH-5.2

CRITICAL

Is the audit-log retention configured to support breach investigation (six years from creation or last in effect)?

Evidence `retention_policy_uri` Gate `retention_minimum_6yr`

☐ Yes ☐ No ☐ N/A

Scoring

Scoring:

- All "critical" items must PASS for `gate.hipaa_for_ai` to PASS.
- This pack is opinionated: in healthcare, "almost compliant" is not compliant. Beacon will not soften the threshold.