AI evidence and retention matrix

Healthcare security engineers, privacy teams and internal audit

Read the complete guide on aona.ai

Define the evidence you need before deciding how long to keep it. HIPAA requires audit controls and activity review, while its six-year Security Rule documentation requirement does not automatically set the retention period for every AI prompt or event. Different records need different decisions.

Use the record type to choose a retention owner and rationale. The example deliberately avoids assigning an invented organisation-wide retention period.

Synthetic records and evaluation plan. No production event, six-year prompt policy or completed deletion is asserted.

Your review

Reviewer: _____ Date: _____

Organisation or team: _____

☐ **Check what the event means**

Identify what an action value proves and which unsupported or unobserved paths it does not cover.

☐ **Record the retention rationale**

Distinguish required policy documentation from prompt content, operational events and exported copies.

☐ **Compare source and export**

Run an authorised synthetic test and record actual fields, timestamp behaviour and access boundaries.

Checked items record your review, not a compliance approval or an installed-product test result.

Notes and next actions

Decision and scope: _____

Evidence to collect: _____

Owner and next review date: _____

Review matrix

Record	Evidence purpose	Retention decision
Security event: synthetic upload	Which application, policy and action were involved?	Security and privacy owners define the period and supported fields.
Policy version and required procedure	What rule and procedure were in effect?	Apply the Security Rule documentation requirement where applicable.

Record	Evidence purpose	Retention decision
Activity-review record	Who reviewed the defined event scope and what followed?	Determine whether it is required Security Rule documentation and apply the relevant rule.
Underlying patient record	Clinical or administrative source of the input.	Use the medical-record and other applicable requirements, not the event-log default.
Exported event copy	Investigation or reporting in another system.	Assign the receiving owner and its access, retention and preservation rules.
Record subject to preservation	Evidence relevant to a specific dispute or investigation.	Resolve the preservation obligation before routine deletion.

A record has a purpose

- **TEST-AI-001:** Synthetic sensitive-input check

Observed outcome: not run

- **Policy reference:** Identify the version that should apply
- **Review reference:** Record who examined the actual evidence

Synthetic event specification

Event reference: TEST-AI-001
Input: an invented administrative note
Application: named by the evaluator before the test
Policy: sensitive-input test policy
Intended outcome: the agreed policy action
Observed outcome: not run
Raw patient content required in the event: no real patient data in this fixture

This is an evidence specification, not a representation of an Aona export schema. Map it to fields actually supported by the selected configuration.

Sources and scope

Sources checked 2026-09-21. Review the current requirements and your actual agreement before using this workbook for a real decision. General information; no professional approval or installed-product result is represented. Confirm the available fields and configured retention. Aona is not a complete medical-record system or a guaranteed HIPAA archive.

HHS: Summary of the HIPAA Security Rule. Audit controls, information-system activity review and retention of required Security Rule documentation.

HHS: Guidance on risk analysis. Identifying and documenting risks to ePHI across the regulated entity’s systems.