NuWyre Records Retention Policy

Effective date: *to be filled at signing* **Version:** v1.0 (subject to attorney revision)
Custodian of record: Jeremy Fish, Founder & CEO, NuWyre, Inc.

---

1. Purpose and authority

This Records Retention Policy ("Policy") governs the retention, preservation, and disposition of records created and maintained by NuWyre, Inc. ("NuWyre") in the regular course of its business as an evidence-layer service provider for customer-facing AI agents. NuWyre captures, integrity-anchors, and stores records of customer-side AI agent interactions under contractual agreements with customer organizations ("Customers").

This Policy is designed to satisfy:

- The business-records exception of the Federal Rules of Evidence, Rule 803(6), establishing that records created in the regular course of business are admissible as evidence of the matters they assert.
- The Telephone Consumer Protection Act ("TCPA") regulatory framework administered by the FCC at 47 C.F.R. § 64.1200, governing consumer consent records for telemarketing communications. Operative retention is also informed by the four-year federal statute of limitations at 28 U.S.C. § 1658(a); industry practice is to retain consent records for at least five years to provide a litigation buffer against late-arising claims.
- The Health Insurance Portability and Accountability Act ("HIPAA") record-retention rules at 45 C.F.R. § 164.530(j) (Privacy Rule documentation; six-year retention) and 45 C.F.R. § 164.316(b)(2) (Security Rule documentation; six-year retention from creation or last effective date), jointly governing protected-health-information access logs, authorization records, and Security Rule policies/procedures.
- SOC 2 Type II audit trail retention norms (seven-year retention).
- State-level record-retention requirements that exceed federal floors, including but not limited to:

    - California Consumer Privacy Act ("CCPA") consumer-request response records (24-month minimum per Cal. Civ. Code § 1798.130).
    - New York medical records retention (six years from last treatment date for adult records; until age of majority + six years for minor records per 10 N.Y.C.R.R. § 405.10).
    - Illinois Biometric Information Privacy Act ("BIPA") consent records (three years following the last interaction with the data subject per 740 ILCS 14/15).
    - State statute-of-limitations windows for malpractice (typically two to ten years across jurisdictions) and financial-services claims (typically three to ten years across jurisdictions).

The customer's declared regulatory regime and jurisdiction(s) of operation determine the **operative minimum** retention period for that customer's records. "Regulatory minimum" in this Policy means the longest applicable requirement across federal AND state law for the customer's regulatory context.

---

2. Records covered

This Policy applies to records created by the NuWyre evidence-layer service, including:

- **Event records:** structured logs of customer-side AI agent interactions captured by NuWyre adapters or direct API ingestion. Each event record includes the agent identifier, timestamp, content (subject to redaction; see § 6), classification labels, and a SHA-256 content hash.
- **Hash chain records:** per-session event ordering integrity records, in which each event's `event_hash` includes the previous event's hash as one of its inputs, forming a tamper-evident linked structure.
- **Daily root records:** per-customer Merkle roots aggregating that day's event hashes, anchored externally via OpenTimestamps (Bitcoin blockchain), RFC 3161 timestamp tokens (independent timestamp authorities), and signed Git commits to the public NuWyre/anchors repository.

- **Audio records:** when the customer's adapter captures audio (e.g., voice-channel TCPA call recordings), the audio binary is stored content-addressed in object storage; the corresponding `audio_records` row in the database stores the audio's SHA-256, duration, MIME type, retention class, and a foreign key to the event the audio binds to.
- **Evaluation records:** automated and human-mediated policy-pack-driven assessments of events against compliance rules (e.g., TCPA consent verification, HIPAA disclosure detection). Each evaluation row records the policy pack version, rule identifier, verdict (clean / flagged / uncertain), severity, evaluator model and version, prompt template hash, and (when applicable) cross-validation against an independent evaluator.
- **Notification records:** rule firings, channel dispatches, and audit entries for compliance officer notifications triggered by flagged evaluations.
- **Audit log records:** structured records of every mutation performed against the NuWyre data layer by an authenticated principal (customer-organization users + NuWyre operators), including the action name, actor identifier, timestamp, target row, and (where applicable) before/after snapshots.
- **Evidence export records:** customer-requested bundles aggregating events + evaluations + audio (when included) + legal documents into signed Ed25519 archives. Each export's request, approval, generation timestamp, downloader identifier, and signed-URL retrieval times are logged.
- **Download records:** every retrieval of an evidence bundle or audit-log export, including the requesting user identifier or API key identifier, IP address, user agent, and timestamp.

This Policy does **not** apply to:

- Transient operational telemetry (e.g., HTTP request logs, infrastructure metrics) that does not record customer-side business events.
- Test fixtures and synthetic data used during development.
- Marketing-site visitor records (governed separately by NuWyre's Privacy Policy).

---

3. Retention periods

3.1 Operative minimums by regulatory regime

Regulatory regime	Federal minimum	Citation
TCPA (telecommunications consent)	5 years from creation (industry practice; litigation buffer over 4-year statute of limitations at 28 U.S.C. § 1658(a))	47 C.F.R. § 64.1200 + 28 U.S.C. § 1658(a)
HIPAA (protected health information access)	6 years from creation or last effective date	45 C.F.R. § 164.530(j) (Privacy Rule) + 45 C.F.R. § 164.316(b)(2) (Security Rule)
SOC 2 Type II audit trail	7 years (typical auditor expectation supporting 5+ audit periods of evidence under TSC CC1.x-CC4.x)	AICPA Trust Services Criteria + auditor practice
Default (no specific regime declared)	7 years from creation	NuWyre default policy

3.2 State-level adjustments

Where the customer operates in a jurisdiction with state-level retention requirements that exceed the applicable federal floor, the **state requirement governs**. Examples (non-exhaustive):

- A customer operating in New York under HIPAA: the operative minimum is the longer of the HIPAA six-year period and the New York six-year-from-last-treatment period (typically converges at six years but can extend further for minor-patient records).
- A customer operating in Illinois with BIPA-covered biometric data: BIPA at 740 ILCS 14/15(a) imposes a **maximum** retention ceiling — biometric data must be destroyed within three years of the data subject's last interaction OR within one year of the original collection purpose being satisfied, whichever is **earlier**. This is structurally different from a retention floor: BIPA-covered records MUST be destroyed within the ceiling regardless of any longer federal retention period that might otherwise apply. A NuWyre customer holding BIPA-covered biometric data should configure aggressive retention class (`pii_minimized` or `phi_minimized`) on those records and rely on the retention sweep procedure to enforce the BIPA ceiling.

- A customer operating in California subject to TCPA: the operative minimum is the longer of the TCPA five-year period and the CCPA 24-month-from-response period (TCPA controls in this case).

The customer's NuWyre service agreement records the customer's declared regulatory regime and jurisdiction(s). The operative minimum is computed from those declarations.

3.3 Customer-configurable extensions

Customers may configure a retention period **above** their operative minimum through the customer organization's Settings surface (admin-role required; portal-facing surface deferred to V2+; current V1 path is via NuWyre operator request). Customer-configured retention periods are recorded in the `customers.default_retention_days` column and validated at every mutation that touches the retention period.

Customers **may not** configure a retention period **below** the operative minimum. The Settings surface and any operator-mediated change request are validated against the operative minimum before persistence.

3.4 Litigation hold

When NuWyre or a Customer receives a litigation hold notice, demand letter, subpoena, or other reasonably foreseeable demand for records, the affected records are flagged with `retention_class = 'litigation_hold'`. Records under litigation hold are **excluded from retention sweep** regardless of any otherwise-applicable retention period. Litigation holds are released only by written direction from counsel.

---

4. Disposition procedure

4.1 Retention sweep cadence

Operational status (as of v1.0 draft): the retention sweep automation is documented infrastructure scheduled to ship in a subsequent Phase 5+ session. The `retention_sweeps` audit table is in place to record sweep executions; the sweep job itself is target-state. Until the sweep job ships, retention is enforced via the append-only-ledger + redaction tombstones + `legal_hold` retention-class flag described in §§ 4.2-4.3 and § 6.

Target-state cadence (Phase 5+ deliverable): NuWyre will run the retention sweep job nightly at 02:00 UTC. The sweep will:

1. Identify records whose `created_at + retention_period < now()`, excluding records flagged with `retention_class = 'litigation_hold'` and records flagged with active customer-extension overrides.
2. Apply the redaction tombstone pattern (described in § 6) to records that have reached their retention period: `events.content` is replaced with the redaction-tombstone marker while `events.content_hash`, `events.event_hash`, and chain integrity remain intact. For records with attached audio binaries, the audio binary file in object storage is removed; the `audio_records` metadata row preserves the audio's SHA-256 fingerprint so the chain remains verifiable.
3. Audit-log entries recording each sweep action are persisted. The audit log itself is retained for the longest applicable retention period (see § 4.2).

Hash chain integrity is preserved across the retention sweep because the chain math depends on `events.event_hash` (computed at ingestion from `events.content_hash`), which is itself preserved through the sweep. Verification of historical bundles remains successful against post-retention chains because the chain reconstruction does not require the (now-redacted) original content.

4.2 Audit trail

Every retention-sweep action — soft-delete, grace-period start, hard-delete — produces an `audit_log` row recording the action, the affected record identifier, the retention period applied, the regulatory regime under which retention was applied, and the operative minimum at the time of action. The audit log itself is retained for the **longest applicable** retention period across all regulatory regimes the customer is subject to.

4.3 Audio binaries

Audio binaries follow the same retention period as their bound event records. When an event is soft-deleted under retention sweep, the corresponding audio binary's `audio_records` row is soft-deleted simultaneously and the underlying audio file in object storage is removed at hard-delete time. The audio's SHA-256 fingerprint persists in the chain via the bound event's hash, so verification of historical bundles that referenced the audio retains its integrity claim even when the audio binary itself is no longer retrievable.

4.4 Evidence bundles

Evidence bundles generated under customer export requests are retained for the **operative minimum** applicable to the bundle's contents (i.e., the longest retention period among the records the bundle includes). When the bundle expires, the bundle archive in object storage is removed; the `evidence_exports` row and its `audit_log` traces are preserved for the audit-log retention period.

---

5. Customer responsibilities

Customers using the NuWyre service represent and warrant that:

- The customer has accurately declared its regulatory regime(s) and jurisdiction(s) of operation in the NuWyre service agreement.
- The customer has obtained all consents and permissions required by applicable law (including but not limited to TCPA consent, HIPAA business associate agreements, and any state biometric or recording disclosure requirements) for the records the customer submits to the NuWyre service.
- The customer will notify NuWyre promptly upon any change in its regulatory regime, jurisdiction(s), or in the scope of records being submitted.
- The customer will notify NuWyre promptly upon receipt of any litigation hold, subpoena, or demand letter affecting records held by NuWyre on the customer's behalf.

---

6. Redaction and tombstone semantics

NuWyre supports two forms of redaction:

- **Operator-initiated redaction** within the admin cockpit: a NuWyre operator, acting at the customer's written request or under compliance review authority, can mark a specific event row as `redaction_applied = true`. The event's `content` field is replaced with the redaction tombstone marker; `events.content_hash` and `events.event_hash` are preserved unchanged (so the chain remains intact). A row is inserted into the `redactions` table recording the original content hash + the regulatory basis.

- **Per-event retention_class:** events can be tagged with `pii_minimized` or `phi_minimized` retention classes that apply different content-handling rules (e.g., aggressive auto-redaction of sensitive content from indexed copies).

Redactions are always logged with a regulatory basis (persisted to the `redactions.reason` column, which is `NOT NULL`-enforced at the database column-constraint level). The operator-facing form field is named `regulatory_basis` and is mapped to `redactions.reason` at the server-action layer. Redaction without a regulatory basis is rejected at the application layer (Zod input validation) AND at the database layer (column NOT NULL constraint).

---

7. Custodian of records

Pursuant to FRE 803(6) and the corresponding state-court business-records doctrines, NuWyre identifies the following individual as the Custodian of Records for the NuWyre evidence-layer service:

- **Name:** Jeremy Fish
- **Role:** Founder & CEO, NuWyre, Inc.
- **Scope of custody:** all records created and maintained by the NuWyre evidence-layer service in the regular course of NuWyre's business.

The Custodian of Records is authorized to execute a business-records affidavit (the Custodian Declaration template; see companion document `/docs/legal/custodian-declaration-template.md`) attesting that NuWyre's records are created automatically, contemporaneously with the events they record, in the regular course of NuWyre's business as an evidence-layer service provider.

---

8. Policy review

This Policy is reviewed at least annually and following any of:

- A change in NuWyre's service offering that materially expands the scope of records captured.
- A change in applicable regulatory minima (federal or state).
- A litigation event or compliance audit that surfaces policy gaps.

Policy review entries are recorded in NuWyre's institutional records and made available to Customers upon written request.

---

9. Signature

Custodian signature: _____

Date: _____

Witness signature (optional): _____

Witness date: _____

Document control

- **Version:** v1.0 (draft; subject to attorney revision)
- **Last updated:** 2026-05-13
- **Next scheduled review:** within twelve (12) months from effective date
- **Drafted by:** NuWyre, Inc.
- **Attorney revision status:** pending; budget line ~$2,000-$5,000 per substantive review per docs/build-plan.md v3.1.7
- **Distribution:** published at `https://nuwyre.com/legal/records-retention-policy.pdf`; included in every NuWyre evidence-bundle export's `legal/` subdirectory starting with the first export generated after the effective date.