Global Authenticity and Operational Evidence Infrastructure: A Framework for Material Risk Verification and Corporate Compliance in Healthcare Markets

Bounded Verification, Chain-of-Custody, and Evidence-Linked Review for Product, Prescription, Dispensation, and Claim Workflows

(Non-Normative)

This submission presents an integrated operational evidence framework for verifiable provenance and material risk management within the life sciences and healthcare sectors. It details an auditable cryptographic architecture designed to mitigate supply chain liabilities and corporate fraud, while upholding U.S. market integrity, financial transparency, and investor protection standards.

Submission to the U.S. Securities and Exchange Commission (SEC)
Date: March 20, 2026

"*An operational blueprint for linking medical supply chain provenance with cryptographic auditability and corporate compliance standards.*"

Cover Letter

To: The U.S. Securities and Exchange Commission (SEC)

Date: March 20, 2026

Subject: Submission of the Healthcare Operational Evidence and Compliance Framework

Dear Sir/Madam,

I am pleased to submit the attached framework, detailing a cross-domain operating model for the cryptographic traceability of medicines, health products, and clinical decisions, for your review.

While healthcare operations are traditionally overseen by medical and food regulatory bodies, the financial materiality of these operations falls directly under the SEC's jurisdiction. Publicly traded pharmaceutical companies, hospital networks, and medical distributors face severe market capital risks tied to supply chain fraud, delayed recall disclosures, and compliance breaches.

This submission provides the SEC and its examiners with an "auditor-ready" infrastructure designed to enforce corporate transparency and protect shareholders. The application of this framework guarantees compliance and prevents financial risks through:

- **Financial Risk Mitigation:** By establishing Immutable Log Segments (ILS) for product provenance and recalls, the framework eliminates the ability of corporate officers to obscure or delay the reporting of material liabilities (such as product safety failures) to investors.
- **M&A and Audit Transparency:** The standardized, non-destructive evidence packs ensure that during mergers, acquisitions, or routine audits, regulators and acquiring entities have mathematically verifiable proof of a target company’s historical compliance and hidden liabilities.
- **Revenue Integrity:** The framework explicitly links financially consequential workflows—such as reimbursements and supply chain settlements—to cryptographically authenticated clinical and product milestones, preventing the artificial inflation of corporate revenues and accounting fraud.

As the healthcare sector becomes increasingly digital and complex, ensuring that corporate disclosures match operational reality is vital for market integrity. This framework equips regulatory authorities with the high-fidelity, bounded-access tools necessary to verify compliance without disrupting institutional workflows.

I look forward to discussing how this operational evidence layer can help the SEC uphold investor protection, fair markets, and transparent capital formation in healthcare.

Sincerely,

/s/ Daniel Bruno Corvelo Costa

Proponent & Lead Architect

Table of Contents

Global Authenticity and Operational Evidence Infrastructure: A Framework for Material Risk Verification and Corporate Compliance in Healthcare Markets

Bounded Verification, Chain-of-Custody, and Evidence-Linked Review for Product, Prescription, Dispensation, and Claim Workflows

(Non-Normative)

Document Status: Non-Normative Implementation Guidance
Companion to: Baselines A–D (Mandatory); Baseline E (Optional, Payments & Settlement)
Scope: Cross-Domain Operating Model — Medicines, Health Products, Clinical Decisions
Audience: Manufacturers, Distributors, Pharmacies, Hospital Systems, Clinical Operators, Benefit Administrators, Auditors, Reviewers, Supervisory Readers

---

> *"The objective of this framework is to make product authenticity, provenance, authorization, and proof-of-safety states evidentiary, replayable, and governable. It does not determine medical truth, regulatory approval, legal liability, or clinical correctness by decree and does not replace physicians, pharmacists, regulators, laboratories, or institutional review; it provides an operational evidence layer that allows product, prescription, dispensation, and high-impact clinical-decision states to be independently reconstructed, verified, escalated, preserved, corrected, and reviewed under bounded access conditions."*

---

0. Executive Summary

0.1 What Problem This Addresses

Medicines, health products, and clinical decisions increasingly traverse fragmented digital and institutional workflows — from manufacturing and packaging through multi-party distribution chains, pharmacy dispensation systems, hospital ordering platforms, clinical decision-support engines, and benefit-administration pipelines. At each handoff, critical operational states — product authenticity, provenance integrity, prescriber authority, dispensation correctness, and safety-relevant evidence — are either asserted without auditable backing, recorded in incompatible formats, or left entirely undocumented. The consequences are tangible and recurring:

Counterfeit and Substitution Risk. Products enter supply chains with incomplete or non-verifiable provenance. When authenticity cannot be reconstructed from evidence artifacts — manufacturer origin, batch/lot linkage, custody handoff records, storage-condition integrity — counterfeit, diverted, or substituted products may reach dispensation without detection. Current detection depends heavily on post-hoc inspections, tip-based investigations, or end-point laboratory testing, none of which scale to the volume and velocity of modern pharmaceutical distribution.

Authorization and Prescription Fragmentation. Prescriptions, clinical instructions, and authorization artifacts are frequently recorded in formats that cannot be independently verified for issuer legitimacy, scope validity, time-window currency, or revocation status. A prescription issued by a prescriber whose authority has lapsed, or whose scope does not extend to the dispensed product, or whose instruction has been superseded by a correction, may proceed through dispensation pipelines without triggering a reconciliation break — because no reconciliation framework exists at the operational layer.

Chain-of-Custody Gaps. Medicines and health products transit through multiple custodial entities: manufacturers, logistics providers, regional distributors, wholesale intermediaries, pharmacy warehouses, hospital receiving docks, unit-dose repackagers, and dispensation counters. At each transition, custody state may change without generating evidence artifacts that are content-addressed, immutable, and linked to the preceding custody record. Stale custody evidence, undocumented custody gaps, and missing handoff confirmations create contamination and substitution risk patterns that are operationally invisible until a downstream incident surfaces.

Opaque Clinical-Decision States. High-impact clinical decisions — dose calculations, contraindication assessments, formulary selections, treatment-protocol outputs — increasingly involve algorithmic or decision-support systems whose outputs are recorded without sufficient context for independent reviewer reconstruction. When a clinical-decision output cannot be replayed against the evidence state that existed at the time of the decision, reviewers are forced to accept the output at face value or reject it entirely. Neither approach is operationally sound.

Review and Dispute Friction. Disputes, recalls, corrections, and supervisory reviews require replayable evidence: the ability to reconstruct what product was involved, where it came from, who authorized its movement or use, under which scope and time window, what safety-relevant evidence existed, and whether downstream release, dispensation, reimbursement, or review actions bound to the correct current-reference state. Without standardized evidence artifacts, content-addressed manifests, break taxonomies, and tiered reviewer access, these reconstruction efforts are slow, incomplete, and inconsistently documented.

Financially Consequential Release Without Sufficient Evidence. Where claim, reimbursement, or payout workflows are in scope, release decisions may proceed on materially unresolved evidence states — unauthenticated products, expired authorizations, unreconciled custody records, or superseded safety evidence. Evidence-linked settlement confirmation, as established in baseline frameworks, provides the operational pattern: financially consequential actions should not proceed when evidence states are materially unresolved.

This framework addresses these operational problems by providing an examiner-ready, institution-usable operating model that treats product authenticity, provenance, authorization, custody,

dispensation, and proof-of-safety as operationally evidenced states subject to reconciliation, correction, preservation, and bounded review — rather than as opaque assertions accepted on trust.

0.2 Why Provenance, Prescription Legitimacy, Dispensation Integrity, and Bounded Verification Must Be Reviewed Together

Conventional approaches address these concerns in isolation: anti-counterfeit programs focus on product verification at point of dispensation; prescription monitoring programs track controlled substances through separate databases; supply-chain serialization initiatives capture custody events without linking them to authorization or safety states; clinical decision-support systems operate within their own evidence ecosystems. Each silo produces evidence artifacts in incompatible formats, maintains separate reconciliation cadences, applies inconsistent break classification logic, and generates review outputs that cannot be cross-referenced without manual reconstruction.

The operational problem is structural. Product authenticity evidence that cannot be linked to custody chain evidence cannot prove that the authentic product at origin is the same product at dispensation. Prescription validity evidence that cannot be cross-referenced against issuer authority evidence and product provenance evidence cannot demonstrate that the authorized prescriber directed dispensation of the correct product within the correct scope. Dispensation records that cannot be linked to upstream custody evidence and downstream claim evidence cannot support reimbursement decisions with confidence.

This framework integrates these concerns into a unified evidence model — not by merging databases, creating universal identifiers, or centralizing PII, but by establishing common artifact structures, reconciliation disciplines, break taxonomies, tiered reviewer access patterns, and governance controls drawn from baseline frameworks that have been developed for analogous operational challenges in tokenized securities and institutional compliance infrastructure.

0.3 What This Document Is and Is Not

What It Is:

- A non-normative, examiner-ready, institution-usable operating model for product authenticity, provenance, authorization, custody, dispensation, proof-of-safety, and optional claim/reimbursement evidence in medicines, health products, and clinical decisions.
- A cross-domain application of evidence, reconciliation, provenance, bounded verification, governance, and optional payment/reimbursement evidence patterns established in baseline frameworks.
- Designed for use by manufacturers, distributors, pharmacies, hospital systems, clinical operators, benefit administrators, auditors, reviewers, and supervisory readers without becoming a legal treatise, medical-practice manual, or patient-facing guide.

What It Is Not:

- Not a universal identity system, centralized PII registry, or medical surveillance architecture.
- Not a hospital ERP specification, pharmacy management system design, or electronic health record redesign.

- Not a prescription-law opinion, pharmacovigilance-only paper, clinical efficacy document, or treatment guideline.
- Not a public-health manifesto, political posture, or replacement for physicians, pharmacists, laboratories, regulators, insurers, or institutional review.
- Not a vendor-locked specification. No references to specific hospitals, pharmacies, insurers, manufacturers, AI models, cloud vendors, devices, or platforms.

0.4 How This Document Builds on Baseline Frameworks

This framework operationalizes concepts and artifact structures from four mandatory baselines and one optional baseline:

The vocabulary, artifact structures, role taxonomy, tiered supervision model, purpose-limitation

Baseline	Role in This Framework
A — Ownership Integrity & Reconciliation Pack	Evidence Set architecture, reconciliation break taxonomy, hold-only containment, offboarding proof bundles, examiner query patterns, content-addressed manifest conventions
B — Operationalization & Conformance Track	Playbook structure, reference implementation profiles, conformance testing, governance charters, RACI conventions, incident coordination, change control, tiered supervisory access
C — Operational Assurance Artifacts Addendum	Evidence Pack manifest templates, logging taxonomy, examiner query packs, RACI matrices, liability trigger catalogs, tiered access purpose-limitation workflows
D — Programmable Privacy & ZKP Framework	Tiered disclosure ladder (Tier 0/1/2), proof-carrying compliance artifacts, freshness/revocation discipline, Verifier Output Pack conventions, bounded verification, purpose codes, TTL bands
E — Payments & Settlement Constitution (Optional)	Settlement evidence production, precondition gates, escrow state models, failure-mode containment, evidence-linked settlement confirmation, intraday liquidity controls

principles, TTL constraints, recertification cadence, and material change governance established in these baselines are reused throughout this document without modification. Where new constructs are introduced for healthcare-specific contexts, they are explicitly labeled as companion-layer additions and remain non-normative.

0.5 Core Thesis

> *"In healthcare-adjacent digital infrastructure, the core operational problem is not only whether a medicine or decision exists, but whether institutions can reliably reconstruct what product was involved, where it came from, who authorized its movement or use, under which scope and time window, what safety-relevant evidence existed, and whether downstream release, dispensation, reimbursement, or review actions bound to the correct current-reference state."*

0.6 Primary Deliverables (This Document)

#	Deliverable	Sections
1	Product Authenticity and Provenance Operating Model	Section 4

#	Deliverable	Sections
2	Prescription, Authorization, and Issuer Legitimacy Model	Section 5
3	Chain-of-Custody, Storage, and Controlled Dispensation Integrity	Section 6
4	Proof-of-Safety and Context-Bound Clinical Decision Evidence	Section 7
5	Review, Recall, Quarantine, Correction, and Supersession Workflows	Section 8
6	Evidence Artifacts, Manifests, Reconciliation, and Preservation	Section 9
7	Tiered Reviewer, Institutional, and Examiner Access	Section 10
8	Governance, Change Control, Recertification, and Accountability	Section 11
9	Financially Consequential Workflows (Optional/Conditional)	Section 12
10	Offboarding, Legacy Compatibility, and Reversibility	Section 13
11	Examiner Readiness: Checks Pack + Query Pack	Section 14
12	Worked Examples (Paste-Ready)	Section 15

0.7 How This Reduces Supervisory and Review Friction

Reviewers, auditors, institutional operators, and supervisory readers conducting oversight of medicine provenance, prescription integrity, dispensation correctness, or clinical-decision safety face friction when:

- Evidence formats vary across participants, requiring custom interpretation for each manufacturer, distributor, pharmacy, or hospital system.
- Reconciliation procedures lack standardization, making break detection inconsistent across product categories and institutional boundaries.
- Product provenance timelines cannot be replayed due to missing custody linkage or incomplete immutable logs.
- Authorization and prescription records operate without clear interfaces to product provenance or dispensation evidence.
- Recall, correction, and supersession events propagate inconsistently, leaving stale reference states in downstream systems.
- Offboarding procedures lack proof bundles, creating examination gaps during system transitions.

This framework reduces friction through:

Friction Reduction Mechanism	Baseline Analog	Healthcare Application
Standardized Evidence Sets	Ownership Evidence Set (OES) — Baseline A	Product Authenticity Evidence Set (PAES), Authorization Evidence Set (AES), Custody Evidence Set (CES), Safety Evidence Set (SES)
Defined Reconciliation Cadences	Reconciliation Framework — Baseline A	Continuous/event-driven/periodic cadences for provenance, custody, authorization, and safety state alignment
Break Taxonomy and Hold-Only Containment	Break Classification — Baseline A	Product-specific break categories (authenticity breaks, custody breaks, authorization breaks, safety breaks) with severity bands and containment logic
Tiered Reviewer Access	Tier 0/1/2 Model — Baselines B, C, D	Purpose-limited reviewer access with TTL, post-access review, and bounded disclosure for product,

Friction Reduction Mechanism	Baseline Analog	Healthcare Application
		prescription, and safety evidence
Examiner Query Packs	Examiner Query Packs — Baselines A, C	Pre-defined queries for provenance replay, authorization verification, custody alignment, and safety-state validation
Offboarding Proof Bundles	Offboarding Proof Bundle — Baseline A	Comprehensive manifests proving product, authorization, and custody integrity through system transitions

1. Non-Normative Disclaimer & Scope Boundaries

1.1 Scope

This framework addresses product authenticity, provenance integrity, authorization legitimacy, chain-of-custody, controlled dispensation, proof-of-safety, bounded reviewer access, and optional claim/reimbursement evidence for medicines, health products, and clinical decisions. The following topics are in scope:

Product Authenticity and Provenance. Operational evidence models for verifying that a medicine or health product is what it purports to be, originated from the claimed source, and traversed verified custody nodes from manufacture to dispensation. Includes content-addressed provenance manifests, batch/lot linkage logic, and authenticity evidence state definitions.

Prescription, Authorization, and Issuer Legitimacy. Operational evidence models for verifying that a prescription, instruction, or authorization was issued by a legitimate authority, within the correct scope and time window, and has not been revoked, superseded, or expired at the time of dispensation or release.

Chain-of-Custody and Dispensation Integrity. Custody event taxonomies, handoff evidence requirements, storage-state integrity logging, and controlled dispensation logic. Includes custody gap detection, stale custody evidence patterns, and contamination/substitution risk indicators.

Proof-of-Safety and Clinical Decision Evidence. Operational evidence models for recording and preserving safety-relevant states — including product safety profiles, clinical-decision-support outputs, contraindication checks, and high-impact instruction records — in formats that support independent reviewer reconstruction without requiring blind trust.

Bounded Reviewer and Examiner Access. Tiered access models (Tier 0/1/2) with purpose limitation, TTL enforcement, post-access review, and minimization discipline applied to product, prescription, custody, and safety evidence.

Correction, Recall, Quarantine, and Supersession. Hold-only containment, recall state transitions, correction and reclassification pathways, supersession chains, current-reference state determination, and non-destructive preservation of prior states.

Governance and Accountability. Change control, recertification cadence, material change triggers, RACI matrices, liability trigger catalogs, no-master-key posture, and distributed approval disciplines.

Optional Claim and Reimbursement Evidence. Where financially consequential workflows are in scope: evidence-linked release, claim or reimbursement gating, settlement/payout linkage, and hold or segmentation logic for financially unresolved states.

Applicable Use Cases:

- Medicine provenance verification from manufacturer to dispensation point
- Prescription authenticity and contextual validity assessment
- Institutional dispensing authorization and pharmacist verification
- Chain-of-custody verification for medicines, biologics, devices, and health products
- Clinical decision artifact review under minimal disclosure constraints
- Product recall, quarantine, hold, or withdrawal workflows
- Hospital, pharmacy, distributor, or manufacturer review workflows
- Reclassification, correction, supersession, or revocation of product or authorization states
- Reimbursement or claim progression where sufficient evidence linkage exists
- Offboarding and legacy system transitions with integrity preservation

1.2 Explicit Non-Goals

This document explicitly excludes the following:

Excluded Topic	Reason
Universal identity systems, national ID, centralized PII registries	Prohibited by design. Framework centers on product authenticity, provenance, authority, and evidence — not on universal patient or citizen identification
Medical surveillance or population-monitoring architecture	Framework supports institutional review and bounded verification, not pervasive monitoring of patient populations
Hospital ERP specification or general EHR redesign	Framework addresses evidence, reconciliation, and governance layers — not clinical system architecture
Prescription-law opinions or pharmacovigilance determinations	Framework uses "alignment objectives" language. No legal conclusions about medical liability, product approval status, or regulatory permissibility
Vendor-locked specifications	No references to specific hospitals, pharmacies, insurers, manufacturers, AI models, cloud vendors, chains, devices, or platforms
Clinical efficacy, treatment guidelines, or standard-of-care determinations	Framework does not assert medical truth or clinical correctness
Public-health manifesto or health-policy advocacy	Neutral, implementation-focused framing only
Replacement for physicians, pharmacists, laboratories, regulators, or institutional review	Framework provides operational evidence layer; human judgment and institutional processes remain authoritative

Deferred to Existing Institutional Processes:

- Drug approval and marketing authorization determinations remain with competent regulatory authorities.
- Clinical judgment, diagnosis, and treatment selection remain with licensed practitioners operating within institutional governance.
- Pharmacy practice standards, dispensing authorities, and controlled substance scheduling remain with applicable pharmacy and drug regulatory bodies.
- Insurance coverage determinations, benefit eligibility, and claim adjudication remain with benefit administrators operating under applicable regulations.
- Laboratory testing, quality assurance, and product release certification remain with accredited laboratories and quality systems.

1.3 Baseline Anchors and Vocabulary Reuse

This framework creates no obligations beyond those already established by the baseline submissions and applicable institutional governance processes. Every control objective, artifact format, and governance procedure herein is derived from or extends an existing baseline construct. Where a concept from this document is not traceable to a baseline anchor, it is labeled explicitly as a "companion-layer addition" and remains non-normative pending baseline incorporation.

Baseline Terms Reused Without Modification:

Term	Origin	Application in This Framework
Evidence Pack (EP)	Baselines A, B, C	Standardized artifact bundle proving authenticity, provenance, authorization, custody, or safety assertions
EP Delta	Baselines A, C	Incremental evidence artifact documenting a state change (e.g., product reclassification, prescription supersession, custody handoff)
Content-Addressed Manifest	Baselines A, C	Cryptographic hash-linked artifact inventory ensuring integrity and tamper detection
Immutable Log Segment (ILS)	Baselines A, C	Tamper-evident, hash-chained log record capturing operational events with timestamps and actor identifiers
Preservation Bundle	Baselines A, C	Evidence collection for legal hold, incident investigation, recall, or dispute proceedings
Tiered Supervisory Access (Tier 0/1/2)	Baselines B, C, D	Graduated access model: Tier 0 aggregate/statistical, Tier 1 event-triggered with purpose limitation, Tier 2 emergency with dual control and post-access review
Purpose Limitation	Baselines C, D	Constraint limiting evidence access to specified review functions with documented justification
TTL (Time-To-Live)	Baselines C, D	Temporal access window with automatic expiration for reviewer access grants
Post-Access Review	Baselines C, D	Audit procedure following reviewer evidence retrieval to verify purpose compliance and access scope
Hold-Only Containment	Baseline A	Temporary restriction preventing state changes pending reconciliation or investigation
Recertification (Recert) Cadence	Baselines A, B, D	Periodic validation of control effectiveness, participant eligibility, and governance compliance
Material Change Trigger	Baselines A,	Threshold event requiring notification, re-evaluation, and

Term	Origin	Application in This Framework
	B, D	documentation
Break Taxonomy	Baseline A	Classification system for reconciliation mismatches by type, severity, and resolution pathway
No-Master-Key Posture	Baselines A, B	No single-party override capability; all governance actions require distributed, multi-party authorization
Verifier Output Pack (VOP)	Baseline D	Standardized artifact recording proof verification results, freshness timestamps, and revocation status

Healthcare-Specific Additions (Minimal):

New terms introduced in this framework are limited to concepts not addressed in baselines. Each addition is justified by the absence of an adequate baseline equivalent:

New Term	Definition	Justification
Product Authenticity Evidence Set (PAES)	Mapping construct linking product identity, manufacturer origin, batch/lot references, and provenance chain to baseline artifact types (EP, ILS, content-addressed manifests)	No baseline equivalent for product-level (non-securities) authenticity evidence
Authorization Evidence Set (AES)	Mapping construct linking prescription, authorization, or issuer legitimacy records to baseline artifact types	No baseline equivalent for healthcare authorization evidence
Custody Evidence Set (CES)	Mapping construct linking medicine/product custody records, handoff confirmations, and storage-state logs to baseline artifact types	Adapts Ownership Evidence Set (OES) concept from Baseline A to physical product custody
Safety Evidence Set (SES)	Mapping construct linking proof-of-safety records, clinical decision outputs, and safety-relevant assessment artifacts to baseline artifact types	No baseline equivalent for clinical safety evidence
Proof-of-Safety State	Operationally evidenced condition indicating whether sufficient safety-relevant evidence exists to support a release, dispensation, or review decision	Healthcare-specific state category not present in securities baselines
Dispensation State	Operationally evidenced condition recording the controlled release of a medicine or health product to its intended recipient	Healthcare-specific state category adapting "settlement state" logic from Baseline E
Current-Reference State (healthcare context)	The most recent, non-superseded, non-revoked evidence state for a product, authorization, custody record, or safety assessment	Reuses baseline concept; no modification, only domain-specific application

1.4 No New Obligations / No Legal Conclusions Posture

This framework does not:

- Create legal obligations for any party beyond those established by existing institutional governance, applicable regulations, and baseline pilot participation requirements.

- Assert legal conclusions about medical liability, product approval status, standard of care, malpractice, reimbursement entitlement, privacy law, authorship of clinical judgment, or regulatory permissibility.
- Determine whether any specific medicine, health product, clinical decision, or institutional arrangement is permitted, prohibited, or required under applicable law.
- Establish new supervisory bodies, regulatory authorities, or institutional oversight structures unless clearly implied by baseline governance patterns.

"Alignment Objectives" Language. When referencing healthcare-specific regulatory concepts — such as drug authentication, prescription monitoring, pharmacovigilance reporting, clinical decision-support oversight, good distribution practice, or reimbursement eligibility — this framework uses "alignment objectives" framing to indicate operational conformance goals without asserting legal interpretations or creating binding obligations. If a specific healthcare law, drug law, privacy law, reimbursement rule, clinical standard, medical-device rule, or cross-border medical regulation is not explicitly referenced in the baselines, this framework does not cite it.

1.5 Relationship to Existing Product, Clinical, Dispensation, Review, Audit, and Supervisory Processes

This framework is designed to complement, not replace, existing processes:

Existing Process	Framework Relationship
Drug regulatory approval and marketing authorization	Framework does not determine approval status. Provenance and authenticity evidence reference approved product identifiers without asserting or challenging regulatory determinations
Pharmacy practice and dispensing standards	Framework does not prescribe dispensing procedures. Dispensation evidence requirements provide standardized artifact structures for recording dispensation events within existing institutional workflows
Clinical decision-making and medical judgment	Framework does not automate, replace, or override clinical judgment. Proof-of-safety evidence models provide reviewer-safe preservation and replay of decision-state contexts
Quality management and good distribution practice	Framework does not replace quality systems. Custody and provenance evidence requirements provide standardized linkage between quality system outputs and reviewable evidence artifacts
Insurance and benefit administration	Framework does not determine coverage or reimbursement eligibility. Optional claim/reimbursement evidence models (Section 12) provide evidence-linked gating for financially consequential releases
Institutional review boards and ethics committees	Framework does not replace ethics oversight. Governance patterns provide accountability and change control structures compatible with institutional review requirements
Regulatory examination and supervisory oversight	Framework provides examiner-ready artifacts, standardized query packs, and tiered access patterns designed to integrate with existing examination processes

2. Problem Statement: Authenticity, Proof-of-Safety, and Review Friction in Medicines and Clinical Decisions

2.1 Medicines and Health Products Increasingly Move Through Fragmented Digital and Institutional Workflows

The operational landscape for medicines and health products has shifted from relatively linear manufacturer-to-pharmacy supply chains toward complex, multi-party, digitally mediated workflows involving contract manufacturers, third-party logistics providers, wholesale redistributors, group purchasing organizations, central fill pharmacies, mail-order dispensation platforms, hospital integrated delivery networks, and specialty pharmacy channels. Each participant operates its own recordkeeping systems, applies its own evidence standards, and produces artifacts in proprietary formats.

This fragmentation creates three operational consequences directly relevant to product integrity and reviewer access:

Evidence Fragmentation. A single medicine's journey from active pharmaceutical ingredient sourcing through finished product release, distribution, and dispensation may generate evidence artifacts across six or more institutional systems with no shared artifact format, no common content-addressing scheme, and no cross-system reconciliation discipline. The reconciliation break patterns identified in Baseline A — where mismatches between registry records, ledger positions, and custody proofs created examiner friction in tokenized securities — manifest with equal severity when provenance records, custody logs, and dispensation records exist in incompatible systems without reconciliation interfaces.

Authority Fragmentation. Prescribing authority, dispensation authority, and release authority may be established, verified, and recorded in separate systems with no operational linkage. A prescriber's authority may be validated at issuance but never re-verified at dispensation; a dispensation authorization may reference a prescription identifier without confirming that the prescription has not been revoked or superseded; a release decision may proceed without confirming that the releasing authority has current, non-expired credentials for the product category in question.

Review Fragmentation. When a dispute, recall, adverse event, or supervisory inquiry requires reconstruction of what happened, reviewers must manually gather evidence from multiple systems, reconcile timestamps across different clock sources, interpret proprietary log formats, and assemble a timeline without standardized evidence packs, content-addressed manifests, or examiner query packs. The examination burden described in Baseline C — where inconsistent logging and unstandardized evidence formats slowed supervisory review in tokenized securities contexts — is directly analogous.

2.2 Counterfeit, Substitution, Stale-Authority, and Provenance-Break Conditions Create Operational and Safety Risk

Four categories of integrity failure create operational and safety risk in medicine and health product workflows:

Integrity Failure Category	Operational Manifestation	Evidence Gap
Counterfeit product entry	Product enters dispensation pipeline without verifiable provenance linking it to an authorized manufacturer and approved production batch	No content-addressed provenance manifest; no batch/lot linkage to manufacturer evidence; no authenticity evidence set
Product substitution	Authentic product is replaced with different product (different formulation, dosage, or active ingredient) at a custody transition point	Custody handoff records lack content-addressed product identity verification; no integrity check at custody boundary
Stale authority	Prescription, authorization, or release instruction references an issuer whose credentials have expired, been revoked, or been restricted since issuance	No real-time or freshness-window-bounded authority validation at dispensation; no EP Delta recording authority state change
Provenance break	Gap in custody chain where product's whereabouts, storage conditions, or custodial responsibility cannot be documented	Missing or incomplete custody event records; no hold-only containment trigger for unresolved custody gaps

These categories are not mutually exclusive. A provenance break may mask a substitution event; a stale authority condition may enable dispensation of a product that should have been subject to hold-only containment pending re-authorization. The operational significance is that each category requires evidence artifacts — not assertions, inspections, or post-hoc investigations — that can be produced, reconciled, and reviewed in a standardized manner.

2.3 Prescriptions, Instructions, and Clinical-Decision Outputs Are Often Recorded Poorly, Detached from Context, or Not Reviewer-Safe

Prescription records, clinical instructions, and clinical-decision-support outputs occupy a supervisory blind spot in many institutional environments. Three patterns contribute:

Assertion-Without-Evidence. A prescription is recorded as "valid" without linking to evidence artifacts demonstrating that the issuer held appropriate authority, that the authority was current at the time of issuance, that the prescription scope (product, quantity, duration, refill conditions) was within the issuer's authorized practice, and that no superseding or revoking event has occurred. The prescription's operational status is an assertion, not an evidenced state.

Context Detachment. A clinical-decision-support output is recorded as a recommendation or alert without preserving the evidence context — the patient parameters, formulary state, contraindication database version, and algorithmic version — that existed at the time the output was generated. When the output is later reviewed (in a dispute, adverse event investigation, or quality review), the reviewer cannot reconstruct the decision context. This is the clinical analog of the "proof freshness" problem addressed in Baseline D: a compliance proof that cannot be linked to its evidence state at the time of generation is operationally unreliable.

Reviewer Opacity. Clinical-decision artifacts may be stored in formats that are accessible only through the originating system, requiring the reviewer to either access the system directly (creating access scope, purpose limitation, and audit trail concerns) or accept a system-generated summary at face value. Neither approach satisfies the bounded verification discipline established in baseline frameworks, where reviewer-safe outputs are designed to provide sufficient evidence for independent verification without requiring full system access or blind trust.

2.4 Product State, Authorization State, Dispensation State, and Claim/Reimbursement State Are Frequently Conflated

A recurring operational problem in healthcare workflows is the conflation of distinct state categories:

State Category	Operational Question	Why Conflation Creates Risk
Product Authenticity State	Is this the product it purports to be, from the claimed source, in the expected condition?	An authentic product with an invalid authorization should not be dispensed; conflating product authenticity with authorization validity masks authorization failures
Authorization State	Is the prescription, instruction, or release authorization valid, current, and within scope?	A valid authorization for the wrong product should trigger a reconciliation break; conflating authorization validity with product identity masks product mismatch
Dispensation State	Has the product been released to the intended recipient under controlled conditions?	A correctly dispensed product based on a subsequently recalled batch should trigger post-dispensation action; conflating dispensation completeness with ongoing safety state masks recall propagation failures
Claim/ Reimbursement State	Does sufficient evidence exist to support a financially consequential release or payout?	A reimbursed dispensation based on subsequently revoked authorization should trigger adjustment; conflating payment status with authorization currency masks stale-authority claims
Proof-of-Safety State	Does sufficient safety-relevant evidence exist to support the release or dispensation decision?	Safety evidence that has been superseded or classified as stale should prevent new dispensation; conflating historical safety evidence with current safety state masks evidence drift

Baseline frameworks — particularly Baseline A's treatment of ownership state, custody state, and settlement state as operationally distinct categories requiring separate evidence and reconciliation — provide the architectural precedent for maintaining these distinctions.

2.5 Institutions Need Bounded Verification Paths Rather Than Pervasive Disclosure or Blind Trust

The supervision dilemma identified in Baseline D — where examiners require complete, auditable evidence while participants require that sensitive attributes not be pervasively exposed — manifests with equal intensity in healthcare contexts. Three healthcare-specific dimensions amplify the tension:

Patient Privacy. Clinical decision evidence, prescription records, and dispensation logs contain or reference patient health information that is subject to institutional confidentiality policies and alignment objectives regarding health data protection. Pervasive disclosure of these records to reviewers, auditors, or supervisory readers without purpose limitation, TTL constraints, and minimization discipline creates privacy risk.

Commercial Sensitivity. Manufacturer provenance records, distributor pricing arrangements, pharmacy formulary configurations, and benefit administrator adjudication logic may contain commercially sensitive information. Review access must be bounded to the specific evidence required for the review purpose — not expanded to include commercially sensitive attributes that are not relevant to the review question.

Cross-Institutional Complexity. A single dispensation event may involve evidence artifacts from a manufacturer (provenance), a prescriber (authorization), a distributor (custody), a pharmacy (dispensation), a clinical system (safety evidence), and a benefit administrator (claim/reimbursement). Review of the dispensation event may require evidence from all six parties, each operating under different institutional governance, different evidence formats, and different disclosure policies. Bounded verification — where a reviewer can confirm specific operational states without requiring full record disclosure from all parties — is operationally necessary.

The tiered disclosure ladder (Tier 0 / Tier 1 / Tier 2) and proof-carrying compliance artifact patterns established in Baseline D provide the operational framework for this bounded verification. This framework applies those patterns to product, authorization, custody, and safety evidence in healthcare contexts.

2.6 Disputes, Recalls, and Review Actions Require Replayable Evidence, Not Only Screenshots, Ad Hoc Attestations, or Disconnected Logs

When a dispute, recall, adverse event, or supervisory inquiry arises, the operational requirement is evidence replay — the ability to reconstruct the relevant state at a specific point in time from standardized, content-addressed, tamper-evident artifacts.

Current healthcare workflows frequently fall short of this requirement:

Recall Scenarios. A product recall affecting a specific batch/lot requires identification of all dispensation events linked to that batch, all current custody holders, and all downstream claim or reimbursement events. Without content-addressed provenance manifests linking batch/lot identifiers to custody records and dispensation events, recall scope determination depends on manual investigation, partial serialization data, and distributor cooperation — none of which produce auditable, examiner-ready evidence.

Adverse Event Investigation. Investigation of an adverse event requires reconstruction of the product provenance (was the correct product dispensed?), authorization state (was the prescription valid and current?), dispensation conditions (was the correct dose and formulation released?), and safety-evidence state (what decision-support outputs, contraindication checks, or clinical assessments existed at the time?). Without preservation bundles and evidence replay capability, investigators reconstruct timelines from screenshots, email chains, and ad hoc system exports.

Dispute Resolution. Disputes between parties — manufacturer and distributor regarding product integrity, prescriber and pharmacy regarding authorization scope, pharmacy and benefit administrator regarding reimbursement eligibility — require evidence that both parties can independently verify. Without standardized evidence sets, content-addressed manifests, and examiner query packs, dispute resolution depends on each party producing its own version of events in proprietary formats, with no shared reconciliation framework.

The baseline frameworks — particularly Baseline A's reconciliation framework, Baseline C's preservation bundle specifications, and Baseline B's evidence pack playbooks — provide the operational patterns for evidence replay, preservation, and reconstruction. This framework applies those patterns to medicine, health product, and clinical decision contexts.

2.7 High-Impact Release or Reimbursement Decisions Should Not Proceed on Materially Unresolved Evidence States

A design principle carried forward from baseline frameworks — particularly Baseline E's treatment of settlement finality as an evidence-backed condition, not an assertion — applies with direct operational relevance to healthcare:

A dispensation decision should not proceed when the product's authenticity state is unresolved. If provenance evidence is incomplete, custody integrity is unverified, or authenticity evidence fails reconciliation, the operationally sound response is hold-only containment pending resolution — not dispensation followed by post-hoc investigation.

A release decision should not proceed when the authorization state is materially ambiguous. If the prescriber's authority cannot be verified against current credentials, if the prescription's validity window is disputed, or if a superseding instruction may exist, the operationally sound response is escalation to bounded reviewer access — not release based on the most recent cached authorization state.

A reimbursement or payout decision should not proceed when evidence linkage to the dispensation event is materially unresolved. If the dispensation evidence cannot be reconciled with the authorization evidence and the product provenance evidence, financially consequential release creates liability exposure. Evidence-linked settlement confirmation — the pattern from Baseline E — requires that payout progression depend on sufficient evidence state, not on the passage of time or the absence of objection.

A clinical-decision-dependent action should not proceed when the decision's evidence context has been superseded. If the formulary, contraindication database, or decision-support algorithm version referenced by a clinical-decision output has been materially updated since the output was generated, the output's proof-of-safety contribution must be re-evaluated before it supports downstream actions.

These are operational control objectives, not legal requirements. This framework does not determine the specific thresholds, escalation criteria, or hold durations applicable to any particular institutional context. It provides the evidence architecture, reconciliation discipline, break taxonomy, and governance patterns that allow institutions to implement these control objectives within their own operational and regulatory environments.

3. Definitions & Neutral Taxonomy (Baseline-Aligned)

This section defines the operational state categories and evidence constructs used throughout the framework. Definitions are operational — they describe evidence conditions, not legal conclusions. Baseline terms are reused without modification; healthcare-specific additions are minimal and explicitly justified.

3.1 Product Authenticity State

Operational Definition. The product authenticity state is the operationally evidenced condition indicating whether a medicine or health product can be verified as originating from the claimed manufacturer, produced in the claimed batch/lot, and conforming to the claimed formulation and specifications — based on available provenance evidence, content-addressed manifests, and integrity checks.

State Values:

State Value	Meaning	Evidence Requirement	Operational Consequence
VERIFIED	Product identity confirmed against manufacturer origin evidence, batch/lot records, and content-addressed provenance manifest	Complete Product Authenticity Evidence Set (PAES) with all required fields populated and integrity checks passed	Product eligible for downstream custody transfer, dispensation, or release
UNRESOLVED	Product identity cannot be confirmed or denied — evidence is incomplete, stale, or under investigation	Partial PAES with documented gaps; investigation ILS initiated	Hold-only containment pending resolution; no dispensation or release
FAILED	Product identity fails verification — evidence contradicts claimed identity, provenance break detected, or integrity check failed	PAES with failure documentation; Preservation Bundle initiated	Immediate hold; quarantine workflow; incident escalation per severity band
NOT_ASSESSED	No authenticity verification has been performed	No PAES exists	Product may not proceed to dispensation; assessment required before release

Non-Legal Framing. A VERIFIED authenticity state indicates that operational evidence artifacts are complete and consistent. It does not constitute a regulatory determination of product approval, a certification of therapeutic efficacy, or a legal guarantee of product safety. When reviewers assess product authenticity state, they evaluate whether evidence artifacts are present, internally consistent, reconciled against provenance records, and retrievable — not whether the product is approved, safe, or efficacious under applicable law.

Baseline Analog. This state category adapts the "record of ownership" operational definition from Baseline A (Section 2.1), where ownership integrity was defined through evidence completeness rather than legal ownership rights. The same evidence-first, non-legal framing applies.

3.2 Provenance State

Operational Definition. The provenance state is the operationally evidenced condition documenting the complete chain of origin, manufacture, packaging, and distribution-pathway for a medicine or health product — from raw material sourcing or finished-product release through each custody transition to the current holder.

State Values:

State Value	Meaning	Minimum Evidence
COMPLETE	Full provenance chain documented from manufacturer release to current custody holder with no gaps	Content-addressed provenance manifest; all custody handoff records present; storage-condition logs linked
PARTIAL	Provenance chain has documented segments but at least one custody transition lacks evidence	Partial manifest with gap indicators; ILS documenting known coverage and known gaps
BROKEN	Provenance chain contains a confirmed break — a custody transition where evidence is absent, contradictory, or tampered	Break detection report; Preservation Bundle capturing break evidence; hold-only containment triggered
RECONSTRUCTED	Provenance break previously detected has been resolved through investigation and compensating evidence	Original break evidence preserved; reconstruction evidence with approval logs; post-review ILS

Provenance Scope. Provenance state covers the product's physical journey and condition history. It does not extend to clinical efficacy, therapeutic classification, or regulatory approval history. Provenance evidence includes: manufacturer identity and batch/lot reference, packaging and labeling evidence, storage-condition records (temperature, humidity, light exposure where applicable), custody handoff confirmations at each transition node, and content-addressed integrity markers linking each segment to the preceding one.

Baseline Analog. Provenance state adapts the chain-of-custody evidence patterns from Baselines A and B, where custody evidence packs (CEP) documented asset control and segregation, and content-addressed storage (Baseline C) ensured tamper-evident linkage across evidence segments.

3.3 Issuer / Prescriber / Authorizer Legitimacy State

Operational Definition. The issuer/prescriber/authorizer legitimacy state is the operationally evidenced condition indicating whether the entity that issued a prescription, instruction, authorization, or release decision held appropriate authority at the time of issuance — as documented by credential evidence, scope records, and currency checks.

State Values:

State Value	Meaning	Evidence Requirement
CONFIRMED	Issuer's authority verified against current credential evidence; scope, jurisdiction, and role validated; no revocation or restriction detected	Authorization Evidence Set (AES) with credential reference, scope verification, currency check, and revocation status
EXPIRED	Issuer's credentials or authority expired at or before the time of the relevant action	AES with expiry detection record; EP Delta documenting transition from CONFIRMED to EXPIRED
REVOKED	Issuer's authority has been revoked by the credentialing body or governance process	AES with revocation record; ILS documenting revocation event and downstream impact assessment
RESTRICTED	Issuer holds authority but with scope limitations that may affect the specific action (product category, jurisdiction, practice setting, time window)	AES with restriction detail; scope-match verification record
UNVERIFIED	No verification of issuer authority has been performed or verification is pending	No complete AES; assessment pending workflow initiated

Non-Legal Framing. Legitimacy state documents whether operational evidence of authority exists, is current, and is consistent. It does not constitute a legal determination of licensure, a finding of unauthorized practice, or a conclusion about malpractice liability. When reviewers assess issuer legitimacy state, they evaluate the evidence trail — not the underlying legal relationship between the issuer and the credentialing body.

Freshness Requirement. Issuer legitimacy state is subject to freshness discipline inherited from Baseline D's proof freshness model. A legitimacy state confirmed at time T may not be relied upon at time T+N without re-verification if N exceeds the applicable freshness window for the authority type. Default freshness windows are defined in Section 5.4.

3.4 Prescription / Instruction Validity State

Operational Definition. The prescription/instruction validity state is the operationally evidenced condition indicating whether a specific prescription, clinical instruction, or authorization document is current, within its intended scope, and has not been superseded, revoked, or expired at the time of the downstream action (dispensation, release, review, or reimbursement).

State Values:

State Value	Meaning	Key Evidence
VALID	Prescription is current, within scope, issued by confirmed-legitimate authority, not superseded or revoked	Complete prescription record linked to AES; scope-match confirmation; freshness check passed
EXPIRED	Prescription validity window has elapsed	Expiry timestamp in prescription record; EP Delta documenting transition
SUPERSEDED	A newer prescription or instruction has replaced this one for the same	Supersession chain record; pointer to superseding prescription; prior

State Value	Meaning	Key Evidence
	product/patient/scope	state preserved
REVOKED	Prescription has been explicitly revoked by the issuer, a governance body, or a regulatory action	Revocation record with authority reference; ILS documenting revocation event
SUSPENDED	Prescription validity is temporarily held pending investigation, review, or correction	Hold-only containment record; investigation workflow ILS
PARTIAL	Prescription is valid for some components of the intended action but not all (e.g., valid for product but expired for refill count)	Partial validity assessment with component-level detail

Supersession Discipline. Prescription supersession follows the versioning and supersession discipline from Baseline A, where prior ownership states were preserved non-destructively when superseded by corrections. A superseded prescription remains available as historical evidence; its state is preserved in the supersession chain, and the current-reference state points to the superseding document.

3.5 Chain-of-Custody State

Operational Definition. The chain-of-custody state is the operationally evidenced condition documenting the sequence of custodial responsibility for a medicine or health product, including each handoff event, storage period, and condition record from the product's entry into the documented chain through its current custodial position.

State Values:

State Value	Meaning	Evidence Requirement
INTACT	Complete, unbroken chain from entry point to current custodian; all handoff events documented and content-addressed	Custody Evidence Set (CES) with all handoff records, storage logs, and content-addressed linkage
GAPPED	One or more custody transitions lack evidence documentation	CES with gap indicators; gap severity assessment; hold-only containment if gap exceeds materiality threshold
COMPROMISED	Evidence of unauthorized custody event, storage violation, or tampering detected	CES with compromise evidence; Preservation Bundle; quarantine workflow triggered
RECONSTRUCTED	Custody gap previously detected has been resolved through investigation and compensating evidence	Gap evidence preserved; reconstruction documentation with approval chain

Custody Event Taxonomy (Preview). Full custody event taxonomy is provided in Section 6.1. Events include: receipt, handoff, storage-entry, storage-exit, temperature-excursion, repackaging, quarantine-entry, quarantine-release, dispensation, return, destruction, and recall-acknowledgment. Each event generates an ILS record with content-addressed integrity markers.

Baseline Analog. Chain-of-custody state directly adapts the custody evidence and chain-of-custody patterns from Baselines A and B. The "Evidence Equivalence Principle" from Baseline A (Section

2.2) applies: regardless of the underlying recordkeeping architecture, participants must demonstrate auditable authority, replayability, reconciliation integrity, and examiner access.

3.6 Dispensation / Release State

Operational Definition. The dispensation/release state is the operationally evidenced condition recording the controlled transfer of a medicine or health product from a custodial entity to its intended recipient — whether a patient, a clinical unit, a downstream dispensation point, or an authorized consumer — under conditions that link the release to a valid authorization, verified product identity, and intact custody chain.

State Values:

State Value	Meaning	Prerequisites
RELEASED	Product has been dispensed or released to the intended recipient under documented conditions	Product authenticity VERIFIED; authorization VALID; custody chain INTACT; dispensation record generated
HELD	Product is physically available but release is blocked pending resolution of an evidence condition	Hold-only containment active; at least one prerequisite state unresolved or under investigation
RETURNED	Product has been returned by the recipient and re-entered custody chain with documented return event	Return event record; re-custody evidence; product re-assessment triggered
RECALLED	Product has been recalled from the recipient or downstream custody; recall acknowledgment and return documented	Recall event record; acknowledgment evidence; return or destruction confirmation

Settlement Analog. Dispensation/release state is the healthcare analog of settlement state in Baseline E. The principle that settlement finality is an "evidence-backed condition, not an assertion" (Baseline E, Section 0.4) applies directly: dispensation is operationally final when all prerequisite evidence states are satisfied and the dispensation evidence pack is generated — not when the product physically leaves the dispensation counter.

3.7 Proof-of-Safety State

Operational Definition. The proof-of-safety state is the operationally evidenced condition indicating whether sufficient safety-relevant evidence exists to support a release, dispensation, or high-impact clinical decision — as documented by safety evidence artifacts, clinical decision records, contraindication assessments, and any applicable algorithmic or decision-support outputs.

State Values:

State Value	Meaning	Evidence Requirement
SUFFICIENT	Required safety evidence classes are present, current, and internally consistent	Safety Evidence Set (SES) with all required evidence classes populated; freshness checks passed
INSUFFICIENT	One or more required safety evidence classes	SES with gap assessment;

State Value	Meaning	Evidence Requirement
	are missing, stale, or inconsistent	escalation triggered per materiality threshold
SUPERSEDED	Safety evidence was previously sufficient but has been superseded by updated evidence (e.g., new contraindication data, updated formulary, revised clinical protocol)	Supersession record; prior SES preserved; re-assessment required
DISPUTED	Safety evidence is under review, challenged, or subject to conflicting assessments	Dispute record; hold-only containment where applicable; reviewer access workflow initiated

Not a Medical Conclusion. Proof-of-safety state records whether operational evidence artifacts exist and are current. It does not determine whether a product is safe, whether a clinical decision is correct, or whether a treatment is appropriate. Institutions, clinicians, and regulators make safety determinations; this framework provides the evidence layer that supports, documents, and preserves those determinations for independent review.

Evidence Classes Supporting Proof-of-Safety. Detailed evidence classes are defined in Section 7.2. Classes include: product safety profile references, contraindication assessment records, drug interaction screening outputs, clinical decision-support outputs, prescriber clinical notes (where relevant to safety determination), and formulary/protocol version references.

3.8 Product Recall / Quarantine / Hold State

Operational Definition. The product recall/quarantine/hold state is the operationally evidenced condition indicating whether a medicine or health product is subject to containment, restriction, or withdrawal from the supply chain or dispensation pipeline — and, if so, under what authority, scope, and conditions.

State Values:

State Value	Meaning	Governance Requirement
ACTIVE	Product is in normal operational flow; no recall, quarantine, or hold in effect	Standard reconciliation cadence applies
HOLD	Product is subject to hold-only containment pending investigation or resolution	Hold record with authority, scope, and duration; no dispensation or transfer permitted
QUARANTINED	Product has been physically or logically segregated from dispensable inventory	Quarantine record with reason, authority, and conditions for release; segregation verification evidence
RECALLED	Product is subject to recall; downstream holders notified; return or destruction required	Recall notification record; scope determination; acknowledgment tracking; return/destruction evidence
WITHDRAWN	Product has been permanently	Withdrawal record with authority;

State Value	Meaning	Governance Requirement
	removed from supply chain by manufacturer or regulatory action	downstream propagation evidence; disposal or return documentation
RELEASED_FROM_HOLD	Product was previously held and has been released following resolution	Hold release record with resolution evidence, approval chain, and post-release verification

Hold-Only Containment Principle. Inherited from Baseline A: when evidence integrity is uncertain, the operationally sound response is hold-only containment — restricting state changes while preserving all evidence for investigation. Hold-only containment does not imply fault, violation, or deficiency; it is a precautionary operational control. Release from hold requires documented resolution, approval, and post-release verification.

3.9 Correction / Supersession / Revocation State

Operational Definition. The correction/supersession/revocation state records the governance posture of any evidence artifact, authorization, or product state — specifically whether it has been corrected, replaced by a newer version, or invalidated.

State Values:

State Value	Meaning	Preservation Requirement
CURRENT	Artifact or state is the active, authoritative version	Standard reconciliation and recertification cadence
CORRECTED	A correction has been applied; the corrected version is now CURRENT; prior version preserved	Prior version retained with correction EP Delta; correction approval chain documented
SUPERSEDED	A newer version has replaced this artifact or state	Supersession chain maintained; pointer to superseding version; prior content preserved
REVOKED	Artifact or state has been invalidated and may not be relied upon for new actions	Revocation record with authority and reason; revocation propagation to dependent artifacts

Non-Destructive Preservation. From Baseline A: corrections, supersessions, and revocations are never destructive. Prior states are preserved in their original form, linked to the correction or supersession record through EP Delta artifacts, and available for historical reconstruction and examiner replay. Silent overwrites — where a prior state is replaced without generating a correction record — are treated as governance violations.

3.10 Claim / Reimbursement / Settlement State (Where in Scope)

Operational Definition. The claim/reimbursement/settlement state is the operationally evidenced condition recording the progression of a financially consequential event — claim submission, adjudication, reimbursement authorization, and payout execution — linked to underlying product, authorization, dispensation, and safety evidence.

This state category is included only where the optional Baseline E (Payments & Settlement Constitution) is applied to healthcare claim and reimbursement workflows. Where financially consequential workflows are not in scope, this state category may be omitted.

State Values:

State Value	Meaning	Evidence Linkage Requirement
SUBMITTED	Claim submitted for adjudication	Claim record linked to dispensation evidence, authorization evidence, and product provenance evidence
ADJUDICATED	Claim reviewed; determination issued	Adjudication record with determination, linked to reviewed evidence artifacts
APPROVED	Claim approved for reimbursement or payout	Approval record with evidence sufficiency confirmation; all prerequisite states verified
DENIED	Claim denied with documented reason	Denial record with reason code and evidence references; appeal pathway documented
PAID	Payout executed and settlement confirmed	Settlement confirmation linked to approval and underlying evidence chain
HELD	Claim progression suspended pending evidence resolution	Hold record; at least one linked evidence state is unresolved
ADJUSTED	Previously paid claim subject to post-payment correction	Adjustment record with reason, amount, and rebinding to corrected evidence

Evidence-Linked Settlement Confirmation. From Baseline E: financially consequential actions should not proceed when evidence states are materially unresolved. Claim progression from SUBMITTED to APPROVED requires that linked product authenticity, authorization, custody, dispensation, and safety evidence states meet minimum completeness thresholds. The specific thresholds are institutional governance decisions — this framework provides the linkage architecture.

3.11 Current-Reference State vs. Historical Preserved State

Operational Definition. For any evidence artifact, authorization, product state, or reconciliation record, the framework distinguishes between the current-reference state (the most recent, non-superseded, non-revoked version that governs current operational decisions) and the historical preserved state (any prior version that has been superseded, corrected, or revoked but is retained for evidence replay and examination).

Operating Rules:

- Downstream actions — dispensation, release, reimbursement, review — bind to the current-reference state, not to historical states.
- Reconciliation checks verify that downstream actions reference the current version; actions bound to superseded states generate reconciliation breaks.
- Historical states are retained non-destructively per the correction/supersession/revocation discipline (Section 3.9). They are available for examiner replay, dispute investigation, and adverse event reconstruction.

- Supersession chains maintain ordered linkage from earliest to current version, enabling full version history traversal.

Baseline Analog. Directly adapts Baseline A's treatment of ownership state versioning, where registry records maintained version lineage with non-destructive preservation of superseded records and examiner-accessible version history.

3.12 Bounded Reviewer Access vs. Unrestricted Disclosure

Operational Definition. This framework distinguishes between bounded reviewer access — purpose-limited, TTL-bounded, tier-appropriate evidence access with post-access review — and unrestricted disclosure — the release of complete evidence records without purpose limitation, temporal boundary, or access audit.

Operating Principle. Bounded reviewer access is the default. Unrestricted disclosure is never the default in this framework. All reviewer, examiner, auditor, and supervisory access to product, authorization, custody, dispensation, safety, and claim evidence operates under the tiered access model inherited from Baselines B, C, and D:

Access Tier	Default Scope	Access Conditions	Post-Access Requirement
Tier 0 — Aggregate/Statistical	Aggregate counts, pass/fail rates, compliance percentages, coverage statistics	No individual product, prescription, or patient-identifiable data	Standard audit log entry
Tier 1 — Scoped/Event-Triggered	Specific evidence artifacts for identified review purpose within defined time window	Documented purpose code; TTL assignment; pseudonymized references where possible	Post-access review within defined SLA
Tier 2 — Exceptional Reveal	Full evidence access including underlying identity, raw provenance, or patient-linked records	Objective trigger; dual-control approval; strict TTL (default 48h); mandatory post-access review	Post-Access Review Pack (PARP) generated for every event

Optional Proof-Based Verification. Where Baseline D's programmable privacy patterns materially improve bounded access, proof-carrying compliance artifacts may be used to satisfy reviewer queries without exposing underlying evidence. A reviewer may confirm that a product's authenticity state is VERIFIED, that an authorization's legitimacy state is CONFIRMED, or that a proof-of-safety state is SUFFICIENT through verifier output logs — without accessing the raw provenance records, credential details, or clinical decision inputs. This reduces disclosure scope while maintaining reviewer confidence.

---

4. Product Authenticity and Provenance Operating Model

4.1 Canonical Product Objects and Official Product-Reference Anchors

Every medicine or health product within the scope of this framework is identified through a canonical product object — a standardized reference record that anchors all downstream evidence artifacts to a specific product identity, formulation, and manufacturer origin.

Canonical Product Object (CPO) — Minimum Fields:

Field	Description	Source
product_reference_id	Unique identifier for this product-formulation-manufacturer combination	Manufacturer or authoritative product registry
manufacturer_id	Identifier for the manufacturing entity or authorized marketing holder	Manufacturer credential or registry reference
product_description	Standardized description including active ingredient(s), strength, dosage form	Official product reference (alignment objective: product monograph equivalents)
batch_lot_reference	Batch/lot identifier for the specific production run	Manufacturer production records
packaging_reference	Packaging configuration identifier (unit, bundle, case, pallet)	Manufacturer packaging records
production_date	Date of manufacture or final release from production	Manufacturer release records
expiry_date	Product expiry or shelf-life end date	Manufacturer specification
content_address	Cryptographic hash of the canonical product object	Computed at CPO generation; used for tamper detection

Official Product-Reference Anchors. The CPO does not replace existing product identification systems (alignment objective: national drug codes, global trade item numbers, serialization identifiers, or similar product reference standards). It serves as a mapping construct that links institutional product identifiers to the evidence artifacts generated under this framework. Participants maintain linkage tables mapping their internal product identifiers to the CPO reference.

Integrity Rules:

- A CPO is generated once per product-batch-lot-manufacturer combination and does not change after generation. If a correction is required (e.g., erroneous batch reference), a correction EP Delta is generated, the original CPO is preserved as historical state, and a corrected CPO becomes the current-reference version.
- All downstream evidence artifacts — PAES, CES, AES, SES — reference the CPO content_address, ensuring that evidence artifacts are bound to the correct product identity and cannot be misattributed to a different product without generating a tamper-detection alert.

4.2 Provenance Linkage Across Manufacture, Packaging, Handoff, Storage, Transfer, and Release

Product provenance is documented through an ordered sequence of provenance events, each generating an ILS record linked to the preceding event through content-addressed chaining. The provenance chain constitutes the operational proof that the product at any given custody node is the same product that was released from the manufacturing point.

Provenance Event Sequence (Conceptual):

Event Type	Actor	Evidence Artifact Generated	Content-Addressed Linkage
MANUFACTURE_RELEASE	Manufacturer	Production release record with CPO reference, quality release attestation, batch/lot documentation	Genesis event; hash anchors the chain
PACKAGING	Manufacturer or contract packager	Packaging record with unit-level identifiers, aggregation hierarchy, labeling confirmation	Links to MANUFACTURE_RELEASE hash
HANDOFF_TO_DISTRIBUTOR	Manufacturer → Distributor	Handoff confirmation with sender/receiver identity, shipment reference, condition attestation	Links to PACKAGING hash
STORAGE_ENTRY	Distributor warehouse	Storage entry record with location, condition parameters, expected duration	Links to preceding HANDOFF hash
STORAGE_EXIT	Distributor warehouse	Storage exit record with condition summary, any excursion records, next destination	Links to STORAGE_ENTRY hash
HANDOFF_TO_PHARMACY	Distributor → Pharmacy/Hospital	Handoff confirmation with receiving entity verification, product count, condition attestation	Links to STORAGE_EXIT hash
RECEIVING_VERIFICATION	Pharmacy/ Hospital	Receiving record with product identity verification, count confirmation, condition check	Links to HANDOFF_TO_PHARMACY hash

Event Type	Actor	Evidence Artifact Generated	Content-Addressed Linkage
DISPENSATION_RELEASE	Dispensing entity	Dispensation record with recipient reference, authorization linkage, product identity confirmation	Links to RECEIVING_VERIFICATION hash; terminal event in dispensation chain

Each event record is stored as an Immutable Log Segment per Baseline C conventions. The content-addressed linkage ensures that any break in the chain — a missing event, a tampered record, or an out-of-sequence insertion — is detectable through hash verification.

4.3 Content-Addressed Manifests and Immutable Provenance Records

Provenance Manifest Structure. For each product unit (or aggregation level tracked within the framework), a provenance manifest aggregates all provenance event records into a single content-addressed document that can be retrieved, verified, and replayed by reviewers.

Provenance Manifest — Conceptual Schema:

```
provenance_manifest:
  manifest_id: [content_address of manifest]
  cpo_reference: [content_address of Canonical Product Object]
  chain_status: COMPLETE | PARTIAL | BROKEN
  event_count: [integer]
  first_event_hash: [hash of genesis event]
  last_event_hash: [hash of most recent event]
  events:
    - event_type: MANUFACTURE_RELEASE
      event_hash: [content_address]
      timestamp: [UTC]
      actor_id: [pseudonymized or role-based]
      previous_hash: null
    - event_type: PACKAGING
      event_hash: [content_address]
      timestamp: [UTC]
      actor_id: [pseudonymized or role-based]
      previous_hash: [hash of preceding event]
    ... [continued for all events]
  integrity_metadata:
```

```
manifest_generated_at: [UTC]
manifest_content_address: [self-referential hash]
chain_verification_result: PASS | FAIL
```

Immutability and Tamper Detection. Provenance records, once generated, are subject to Baseline C's content-addressed storage requirements: they are stored using cryptographic content hashes as identifiers, cannot be modified after storage without generating a new content address (which would break the chain linkage), and are subject to periodic integrity verification through hash chain validation.

Correction Handling. If a provenance event record contains an error (e.g., incorrect timestamp, wrong actor identifier), the original record is preserved and a correction EP Delta is generated per Section 3.9 conventions. The provenance manifest is updated to reference the correction, and the chain integrity metadata reflects the correction event. The original erroneous record remains available for historical review.

4.4 Authenticity Evidence States and Minimum Replay Requirements

For a product's authenticity state to reach VERIFIED, the following minimum evidence elements must be present, current, and internally consistent:

Minimum Replay Requirements for VERIFIED Authenticity:

Evidence Element	Source	Freshness Requirement	Failure Consequence
Canonical Product Object (CPO)	Manufacturer or product registry	Static (generated once per batch/lot)	If CPO absent or tampered: NOT_ASSESSED
Manufacturer identity verification	Manufacturer credential evidence	Per issuer legitimacy freshness window (Section 5.4)	If manufacturer identity unverified: UNRESOLVED
Batch/lot release documentation	Manufacturer production records	Static (generated at release)	If batch/lot documentation absent: UNRESOLVED
Provenance manifest	Aggregated from provenance events	Updated at each custody event	If manifest BROKEN: FAILED; if PARTIAL: UNRESOLVED
Most recent custody handoff confirmation	Current custodian	Event-driven (generated at each handoff)	If most recent handoff unconfirmed: UNRESOLVED
Content-addressed integrity verification	Hash chain validation	Periodic (per reconciliation cadence)	If integrity check fails: FAILED

Replay Capability. A reviewer must be able to reconstruct a product's authenticity state at any historical point by traversing the provenance manifest, verifying each event's content-addressed linkage, confirming the CPO reference, and checking the manufacturer identity evidence that was current at that point. This replay capability is the healthcare analog of "ownership timeline replay" from Baseline A (Section 11).

4.5 Batch / Lot / Package / Custody-Reference Linkage Logic

Products exist at multiple aggregation levels — individual units, packages, cases, pallets, shipments — and the linkage between these levels must be maintained for provenance integrity, recall scope determination, and dispensation tracking.

Aggregation Hierarchy:

```
Batch/Lot (production level)
  └── Pallet (logistics level)
       └── Case (distribution level)
            └── Package (pharmacy/hospital level)
                 └── Unit (dispensation level)
```

Linkage Rules:

- Each aggregation level references its parent level through a content-addressed pointer. A unit record references its parent package; a package references its parent case; and so on.
- Disaggregation events (e.g., a case is opened and individual packages are distributed to different pharmacies) generate ILS records documenting the disaggregation, the resulting child entities, and the custodial responsibility for each child.
- Aggregation events (e.g., units are repackaged into unit-dose configurations) generate ILS records with linkage to the source package and the resulting aggregation, including any repackaging entity identity and repackaging conditions.
- Recall scope determination traverses the aggregation hierarchy: a batch-level recall identifies all descendant packages and units through the linkage chain, enabling comprehensive downstream notification and containment.

Custody-Reference Linkage. Every custody event (Section 6.1) references both the product aggregation level at which custody was transferred and the provenance manifest segment applicable to that event. This cross-reference ensures that custody evidence and provenance evidence remain aligned and reconcilable.

4.6 Provenance Boundary Tests and Integrity Failure Conditions

Provenance boundary tests determine when enhanced controls are required — following the boundary test pattern established in Baselines A and D.

Provenance Boundary Test Matrix:

Condition	Trigger Threshold	Default Response	Escalation Path
Provenance chain gap detected	Any missing handoff record in chain	Hold-only containment	Tier 1 investigation; Tier 2 if unresolved within SLA
Content-address mismatch in chain	Hash verification failure at any event	Immediate hold; alert	Incident response per severity; Preservation Bundle initiated

Condition	Trigger Threshold	Default Response	Escalation Path
Manufacturer identity evidence stale	Manufacturer credential exceeds freshness window	Block dispensation; re-verification required	Tier 1 if re-verification fails
Storage condition excursion recorded	Temperature, humidity, or light parameter outside specification	Event-driven assessment; hold if excursion exceeds materiality	Product quality assessment per institutional procedures
Repackaging event without authorized repackager	Repackaging entity credentials unverified	Hold-only containment	Tier 1 investigation of repackager authority
Disaggregation without linkage to parent	Child entity cannot be traced to parent aggregation level	Hold-only containment; treat as provenance BROKEN	Tier 1 investigation; potential FAILED authenticity state
Multiple products claiming same serial/unit identifier	Collision detected in unit-level references	Immediate hold on all affected units	Incident response; potential counterfeit investigation
Provenance evidence unavailable for retrieval	Content-addressed artifact not found in storage	Hold-only containment; availability incident logged	Storage recovery procedures per Baseline C

Application Guidance. Scenarios not matching boundary tests follow standard reconciliation cadence (Section 9.5). Multiple boundary tests may apply simultaneously; the most conservative response governs. All boundary test determinations are logged in ILS for reviewer access.

4.7 What Counts as Operationally Verified Product Authenticity vs. Unresolved Authenticity Posture

This section establishes the operational distinction between a product whose authenticity has been verified through evidence and a product whose authenticity remains unresolved. The distinction governs whether the product may proceed to dispensation, release, or claim workflows.

Operationally Verified Product Authenticity (VERIFIED State) Requires:

1. A complete, content-addressed Canonical Product Object (CPO) referencing the specific product-batch-lot-manufacturer combination.
2. A provenance manifest with COMPLETE chain status — no gaps, no integrity failures, no unresolved breaks.
3. Manufacturer identity evidence that is CONFIRMED under the issuer legitimacy model (Section 5) and within the applicable freshness window.
4. The most recent custody handoff confirmation, verified and content-addressed.
5. A passing content-addressed integrity verification on the complete evidence chain.

Unresolved Authenticity Posture (UNRESOLVED State) Exists When:

Any one of the above five elements is absent, stale, under investigation, or fails verification — but no element has actively failed (contradiction, tampering evidence, or counterfeit indicator).

Unresolved posture triggers hold-only containment: the product may not proceed to dispensation or release, but is not quarantined or recalled. Resolution requires completing the missing evidence, refreshing stale evidence, or concluding the investigation with a determination that moves the state to either VERIFIED or FAILED.

Failed Authenticity (FAILED State) Exists When:

At least one evidence element actively contradicts the claimed product identity — provenance chain broken with tampering indicators, manufacturer identity evidence fails verification, content-addressed integrity check detects modification, or other indicators of counterfeit, diversion, or substitution. Failed state triggers quarantine, incident escalation, and Preservation Bundle generation.

Operational Consequence Summary:

Authenticity State	Dispensation Permitted	Transfer Permitted	Claim/ Reimbursement Permitted	Required Action
VERIFIED	Yes	Yes	Yes (if other prerequisites met)	Standard reconciliation cadence
UNRESOLVED	No	Hold-only (no transfer to dispensation)	No	Complete evidence; resolve gaps
FAILED	No	Quarantine only	No; adjustment if previously paid	Quarantine; incident escalation; Preservation Bundle
NOT_ASSESSED	No	No	No	Assessment required before any action

---

5. Prescription, Authorization, and Issuer Legitimacy Model

5.1 Authorization as an Evidenced Operational State, Not a Mere Assertion

In conventional healthcare workflows, a prescription or authorization is frequently treated as a document — something that exists or does not exist, that is presented or not presented. The operational problem is that a document's mere existence does not demonstrate that it was issued by a legitimate authority, within the correct scope, during a valid time window, and has not been superseded since issuance. Authorization-as-document treats authorization as a binary: present/absent. Authorization-as-evidence treats it as a multi-dimensional state: each dimension must be independently verifiable.

This framework models authorization as an operational state composed of independently verifiable dimensions:

Dimension	Operational Question	Evidence Required
Issuer Legitimacy	Did the issuing entity hold appropriate authority at the time of issuance?	Issuer credential evidence (AES); legitimacy state CONFIRMED

Dimension	Operational Question	Evidence Required
Scope Validity	Does the authorization cover the specific product, quantity, duration, and conditions of the intended action?	Scope-match verification record linking authorization parameters to intended action parameters
Temporal Currency	Is the authorization within its validity window and has it not expired?	Timestamp verification; expiry check; freshness confirmation
Revocation Status	Has the authorization been revoked or suspended since issuance?	Revocation check against current revocation records; revocation status CLEAR or REVOKED
Supersession Status	Has a newer authorization replaced this one for the same scope?	Supersession chain query; current-reference state determination
Channel / Context Validity	Was the authorization transmitted through a recognized channel and received by the intended party?	Channel verification record; receipt confirmation

Evidence-First Principle. Each dimension requires an evidence artifact — not an assertion, attestation, or database entry. When an examiner reviews an authorization state, they can independently verify each dimension through the evidence chain rather than relying on a single party's representation that "the prescription is valid."

Baseline Analog. This approach directly adapts Baseline A's treatment of ownership as a multi-component evidence state (Section 2.1), where a "record of ownership" consisted of six independently verifiable operational components rather than a single authoritative assertion.

5.2 Who Can Authorize What, Under Which Role and Scope

Authorization authority is modeled through role-scope-product mappings that define which categories of actors may issue which categories of authorizations for which product categories. This framework does not prescribe specific role definitions — those remain with applicable institutional governance and credentialing bodies — but establishes the evidence structure for documenting and verifying authority claims.

Role-Scope-Product Authority Matrix (Conceptual Template):

Role Category	Authorization Type	Product Scope	Scope Constraints	Evidence Class
Licensed prescriber	Prescription (new, renewal, modification)	Products within prescriber's authorized practice scope	Jurisdiction, practice setting, specialty restrictions	Prescriber credential + scope attestation
Institutional authorizer	Formulary-based release authorization	Products on institutional formulary	Institutional affiliation, formulary version, clinical unit	Institutional credential + formulary reference
Pharmacist / dispenser	Dispensation authorization	Products authorized for dispensation at the dispensation point	Pharmacy licensure, dispensation category restrictions	Dispensation credential + site authorization
Delegated	Prescription under	Products within	Delegation	Delegation record +

Role Category	Authorization Type	Product Scope	Scope Constraints	Evidence Class
prescriber	delegation protocol	delegation scope	instrument, supervising prescriber reference, protocol limits	supervising prescriber AES
Emergency authorizer	Emergency dispensation authorization	Products required for immediate clinical need	Emergency declaration record, time-limited scope, post-hoc review requirement	Emergency authorization record + clinical justification
Recall authority	Recall, withdrawal, or hold authorization	Products subject to safety action	Regulatory authority or manufacturer quality authority	Recall authority credential + safety evidence reference

Non-Prescriptive Framing. This framework does not determine which roles are authorized to perform which actions — those determinations are institutional and regulatory governance decisions. The matrix provides the evidence architecture: for any authorization event, the framework requires that the authorizer's role, scope, and product authority be documented in evidence artifacts that can be independently verified.

Authority Delegation. Where authorization is delegated (e.g., a nurse practitioner prescribing under physician delegation, a pharmacy technician dispensing under pharmacist supervision), the delegation chain must be documented as an evidence chain linking the delegate's action to the delegator's authority. Each delegation link includes: the delegation instrument (protocol, order set, standing order), the delegator's AES (confirming the delegator's authority to delegate), the scope limitations of the delegation, and the temporal validity of the delegation.

5.3 Time-Bounded, Location-Bounded, Channel-Bounded, and Purpose-Bounded Authorization

Authorizations in healthcare are inherently bounded — they do not confer unlimited authority to dispense any product, at any time, in any location, through any channel. This framework requires that authorization bounds be documented as evidence fields and verified at each downstream action.

Authorization Bound Categories:

Bound Type	Definition	Evidence Field	Verification Method
Time Bound	Authorization is valid only within a defined temporal window (issue date → expiry date, or issue date + defined duration)	validity_start, validity_end, duration_limit	Timestamp comparison at time of downstream action; expired authorizations trigger EXPIRED state
Location Bound	Authorization is valid only at specified dispensation locations, within specified jurisdictions, or within specified practice settings	authorized_locations[], jurisdiction_codes[], setting_types[]	Location-match verification comparing dispensation point against authorized locations

Bound Type	Definition	Evidence Field	Verification Method
Channel Bound	Authorization is valid only when transmitted and received through recognized channels (e.g., electronic prescribing network, institutional order system)	authorized_channels[], transmission_record	Channel verification confirming that authorization was received through a recognized pathway
Purpose Bound	Authorization is valid only for specified clinical purposes or patient populations (e.g., specific indication, clinical trial enrollment, compassionate use)	purpose_codes[], population_restrictions[]	Purpose-match verification comparing intended use against authorized purposes
Quantity Bound	Authorization specifies maximum quantities, refill limits, or dosage ceilings	max_quantity, refill_count, dosage_ceiling	Quantity accumulation tracking; threshold breach triggers hold
Product Bound	Authorization is specific to identified product(s) and does not extend to substitutes unless explicitly noted	authorized_products[], substitution_policy	Product-match verification against CPO references

Bound Verification at Dispensation. Before a dispensation event proceeds, each applicable bound must be verified against current conditions. A single bound failure (expired time window, unauthorized location, exceeded quantity) generates a reconciliation break and triggers hold-only containment on the dispensation. The dispensation may proceed only if the bound failure is resolved through re-authorization, correction, or escalated approval per institutional governance.

5.4 Prescription Validity, Renewal, Expiry, Revocation, and Supersession Discipline

Prescription validity is not a static attribute — it is a dynamic state subject to renewal, expiry, revocation, and supersession events, each of which generates evidence artifacts.

Prescription Lifecycle State Machine:

```
ISSUED → VALID → [RENEWED → VALID] → EXPIRED
                ↘ SUSPENDED → [REINSTATED → VALID | REVOKED]
                ↘ SUPERSEDED (pointer to superseding prescription)
                ↘ REVOKED
```

Lifecycle Event Evidence Requirements:

Lifecycle Event	Actor	Evidence Generated	State Transition
Issuance	Prescriber	Prescription record with all bound fields; AES linkage; issuer legitimacy confirmation	→ VALID
Renewal	Prescriber (same or authorized successor)	Renewal record referencing original prescription; updated	VALID → VALID (new validity window)

Lifecycle Event	Actor	Evidence Generated	State Transition
		bounds; fresh AES confirmation	
Expiry	System/automated	Expiry detection record with timestamp; EP Delta	VALID → EXPIRED
Suspension	Prescriber, institution, or governance body	Suspension record with reason and authority; hold-only containment on dependent dispensation events	VALID → SUSPENDED
Reinstatement	Authority that imposed suspension	Reinstatement record with resolution evidence and approval chain	SUSPENDED → VALID
Supersession	Prescriber (issuing replacement)	Superseding prescription record; supersession chain linkage; prior prescription preserved	VALID → SUPERSEDED
Revocation	Prescriber, institution, governance body, or regulatory action	Revocation record with authority and reason; downstream impact assessment	Any active state → REVOKED

Freshness Windows for Prescription Validity:

Authorization Type	Default Freshness Window	Re-Verification Trigger	Rationale
Acute prescription (single-fill)	Valid until filled or expired (per prescription terms)	At dispensation	Single-use; no ongoing freshness concern beyond expiry
Chronic prescription (multi-fill / refill)	Verify at each refill event	Each refill triggers re-check of issuer legitimacy and revocation status	Authority may change between refills
Institutional standing order	Verify per institutional recertification cadence (alignment objective: at least annually)	Recertification event or material change trigger	Standing orders may outlive the authorizing physician's affiliation
Emergency authorization	Valid for defined emergency window only (typically 24–72 hours per institutional policy)	Expiry of emergency window	Time-limited by design; post-hoc review required
Delegated prescription	Verify delegation instrument validity at each dispensation	Each dispensation triggers delegation freshness check	Delegation may be revoked independently of the prescription

Supersession Chain Discipline. Adopted from Baseline A's ownership version lineage: when a prescription is superseded, the framework maintains an ordered chain linking the superseded prescription to its replacement. The superseded prescription's state becomes SUPERSEDED and includes a pointer to the superseding prescription's record. The superseding prescription's record includes a pointer to the superseded prescription. Both are content-addressed and preserved non-destructively.

5.5 Issuer / Prescriber / Institutional Authority Validation

Authority validation is the process of confirming that the entity claiming authorization authority actually holds the claimed authority at the time of the relevant action. This process generates Authorization Evidence Set (AES) artifacts.

AES Minimum Fields:

Field	Description	Source
issuer_reference_id	Pseudonymized or role-based identifier for the authorizing entity	Institutional credential system
credential_reference	Pointer to the issuer's active credential artifact	Credentialing body or institutional records
authority_type	Category of authority claimed (prescribing, dispensing, delegating, recalling)	Credential content
scope_attestation	Documented scope of authority (product categories, practice settings, jurisdictions)	Credentialing body attestation
currency_check_timestamp	Timestamp of the most recent verification that the credential is active and not revoked	Verification process output
revocation_check_result	Result of revocation check (CLEAR, REVOKED, RESTRICTED, UNAVAILABLE)	Revocation list or status registry query
freshness_status	CURRENT, EXPIRING, or EXPIRED relative to applicable freshness window	Computed from currency_check_timestamp and freshness window
evidence_content_address	Self-referential content hash of this AES record	Computed at generation

Validation Workflow (Conceptual):

1. At authorization event (prescription issuance, dispensation authorization, release decision), the system queries for the issuer's current credential status.
2. The credential reference is checked against the applicable revocation list or status registry.
3. The scope attestation is compared against the specific action parameters (product, location, purpose) to confirm scope match.
4. The results are recorded in an AES artifact, content-addressed and stored as an ILS.
5. If validation fails (credential expired, revoked, restricted, or scope mismatch), the authorization state transitions to the appropriate failure value (EXPIRED, REVOKED, RESTRICTED, or UNVERIFIED) and hold-only containment is triggered on dependent downstream actions.

Optional Proof-Based Validation. Where Baseline D's programmable privacy patterns are applied, authority validation may use proof-carrying compliance artifacts to confirm that an issuer satisfies authority requirements without exposing the issuer's full credential details. A verifier output

confirming "issuer holds prescribing authority for product category X within jurisdiction Y" provides bounded verification without disclosing the issuer's identity, license number, or practice address to the dispensation system. The VOP is stored and available for Tier 1 or Tier 2 reviewer access if escalation occurs.

5.6 Authorization-State Diffs and EP Delta Treatment

Authorization states change over time. Each change — renewal, expiry, revocation, suspension, supersession, scope modification — generates an EP Delta artifact documenting the transition.

EP Delta for Authorization State Changes — Structure:

```
ep_delta:
  delta_id: [content_address]
  authorization_reference: [content_address of affected authorization]
  previous_state: [state value before change]
  new_state: [state value after change]
  change_type: RENEWAL | EXPIRY | REVOCATION | SUSPENSION |
               REINSTATEMENT | SUPERSESSION | SCOPE_MODIFICATION
  change_authority: [identifier of entity or process causing change]
  change_timestamp: [UTC]
  change_evidence: [content_address of supporting evidence]
  downstream_impact:
    affected_dispensation_events: [count or list of affected events]
    hold_actions_triggered: [count or list of holds initiated]
    notification_records: [content_addresses of notifications sent]
  previous_delta_hash: [content_address of preceding EP Delta, if any]
  delta_content_address: [self-referential hash]
```

Chaining. EP Deltas for a given authorization form an ordered chain, enabling reviewers to traverse the complete authorization history from issuance through all state transitions. Each delta references the preceding delta through content-addressed linkage, creating a tamper-evident authorization timeline.

Downstream Impact Assessment. When an authorization state changes (especially to REVOKED, SUSPENDED, or EXPIRED), the EP Delta includes a downstream impact assessment identifying dispensation events, claims, or release decisions that were bound to the now-changed authorization. Dependent actions bound to a revoked or expired authorization generate reconciliation breaks requiring investigation and potential adjustment.

5.7 Exceptional Reviewer Access When Authorization Evidence Is Disputed or Incomplete

When authorization evidence is disputed — parties disagree about issuer legitimacy, scope validity, or revocation status — or when evidence is incomplete — credential verification unavailable, revocation list unreachable, or issuer records partially missing — the framework provides structured escalation to exceptional reviewer access.

Escalation Triggers for Authorization Disputes:

Condition	Default Response	Escalation Path
Issuer legitimacy disputed by dispensing entity	Hold-only containment on pending dispensation; AES review initiated	Tier 1: scoped review of issuer credential evidence within TTL window
Prescription scope contested (product, quantity, or indication disagreement)	Hold-only containment; scope-match evidence gathered from both parties	Tier 1: scoped review of authorization bounds and dispensation parameters
Revocation status unavailable (revocation list unreachable)	Conservative FAIL per Baseline D convention; hold-only containment	Tier 1 after defined grace period; Tier 2 if prolonged unavailability
Supersession chain ambiguity (multiple prescriptions claiming current status)	Hold-only containment on all affected prescriptions	Tier 1: supersession chain reconciliation; Tier 2 if conflicting evidence from different institutional sources
Emergency authorization validity challenged post-hoc	Post-hoc review workflow; dispensation evidence preserved	Tier 1: review of emergency declaration evidence and clinical justification; Tier 2 if potential unauthorized dispensation
Delegated authority validity questioned	Hold-only containment on future delegated actions; prior actions preserved for review	Tier 1: review of delegation instrument, delegator AES, and delegation scope; Tier 2 if delegation may have been forged or unauthorized

Reviewer Access Discipline. Even under escalation, reviewer access operates under bounded verification principles:

- Tier 1 reviewers access scoped evidence artifacts (specific AES records, prescription records, scope-match verification results) under documented purpose codes and TTL constraints.
- Tier 2 reviewers access underlying identity or credential details only when Tier 1 evidence is insufficient to resolve the dispute, with dual-control approval, strict TTL (default 48 hours), and mandatory Post-Access Review Pack generation.
- All reviewer access events are logged as ILS records, content-addressed, and subject to post-access audit.

Resolution Outcomes. Authorization dispute resolution results in one of the following:

1. **Authorization confirmed:** AES updated with dispute resolution evidence; hold released; dispensation may proceed.

2. **Authorization corrected:** Correction EP Delta generated; prior authorization state preserved; corrected authorization becomes current-reference.
3. **Authorization revoked:** Revocation EP Delta generated; all dependent dispensation and claim events identified for downstream impact assessment.
4. **Authorization remains unresolved:** If resolution cannot be achieved within governance SLA, the matter escalates to institutional governance (alignment objective: medical staff committees, pharmacy and therapeutics committees, or regulatory authorities as applicable). Hold-only containment remains in effect pending final resolution.

---

6. Chain-of-Custody, Storage, and Controlled Dispensation Integrity

6.1 Custody Event Taxonomy

Every transition in custodial responsibility for a medicine or health product generates a custody event — a discrete, evidence-producing occurrence that is logged as an Immutable Log Segment (ILS), content-addressed, and linked to the preceding custody event through hash chaining. The custody event taxonomy defines the recognized event categories, required evidence fields, and downstream implications.

Custody Event Categories:

Event Code	Event Name	Description	Minimum Evidence Fields
CUS_RECEIPT	Receipt	Product received by a new custodial entity from a transferring entity	Receiving entity ID, transferring entity ID, product CPO reference, quantity, condition attestation, timestamp
CUS_HANDOFF	Handoff	Custody formally transferred between entities with confirmation from both sides	Sender confirmation, receiver confirmation, product reference, handoff conditions, transport reference
CUS_STORAGE_ENTRY	Storage Entry	Product enters a defined storage location with documented conditions	Storage facility ID, location reference, entry conditions (temperature, humidity), expected duration
CUS_STORAGE_EXIT	Storage Exit	Product departs a storage location	Exit timestamp, condition summary for storage period, excursion records (if any), destination reference
CUS_TEMP_EXCURSION	Temperature Excursion	Storage conditions exceeded defined parameters	Excursion start/end timestamps, parameter range, severity classification, remedial action record

Event Code	Event Name	Description	Minimum Evidence Fields
CUS_REPACKAGE	Repackaging	Product repackaged into different aggregation units	Repackaging entity ID, source unit references, resulting unit references, repackaging conditions, authority credential
CUS_QUARANTINE_ENTRY	Quarantine Entry	Product placed in quarantine segregation	Quarantine reason, authority reference, segregation location, expected review timeline
CUS_QUARANTINE_RELEASE	Quarantine Release	Product released from quarantine following review	Release authorization, resolution evidence, post-quarantine condition assessment
CUS_DISPENSATION	Dispensation Release	Product released to intended recipient under controlled conditions	Recipient reference (pseudonymized), authorization linkage, product identity verification, dispensing entity credential
CUS_RETURN	Return	Product returned from recipient or downstream custodian	Return reason, returning entity, product condition assessment, re-custody evidence
CUS_DESTRUCTION	Destruction	Product destroyed under documented conditions	Destruction authorization, method, witness record, disposal evidence, environmental compliance reference
CUS_RECALL_ACK	Recall Acknowledgment	Custodian acknowledges receipt of recall notification and reports affected inventory	Recall reference, affected inventory assessment, containment actions taken, response timeline
CUS_HOLD_ENTRY	Hold Entry	Product placed under hold-only containment pending investigation	Hold authority, reason, scope, affected product references, expected resolution timeline
CUS_HOLD_RELEASE	Hold Release	Product released from hold following resolution	Release authorization, resolution evidence, approval chain

Event Attribute Requirements. Every custody event record must include, at minimum: a unique event identifier, a UTC timestamp synchronized to an authoritative time source, the event code from the taxonomy above, the acting entity identifier (pseudonymized or role-based), the affected product reference (CPO content address and aggregation level), the event outcome, the content address of the preceding custody event in the chain, and the self-referential content address of this event

record. These attribute requirements mirror the minimum event attributes from Baseline C's logging taxonomy (Section A.2).

Event Chaining. Custody events for a given product unit (or aggregation level) form a strictly ordered, content-addressed chain. Each event record contains the content hash of the preceding event, creating a tamper-evident sequence. Any insertion, deletion, or modification of an event record in the chain breaks the hash linkage and triggers an integrity failure alert. This chaining pattern is inherited directly from Baseline C's Immutable Log Segment architecture.

6.2 Storage-State Integrity and Transition Logging

Medicines and health products are frequently condition-sensitive — their safety and efficacy depend on maintenance of specified storage conditions throughout the custody chain. Storage-state integrity addresses the evidence requirements for documenting that storage conditions were maintained, and for recording and assessing deviations.

Storage-State Evidence Requirements:

Evidence Element	Content	Generation Trigger	Freshness
Storage condition baseline	Defined acceptable ranges for temperature, humidity, light, and other relevant parameters for the product category	Established at CPO generation from product specifications	Static per product specification; updated only on product re-specification
Continuous condition log	Periodic readings of actual storage conditions at the storage facility	Automated sensor readings at defined intervals (alignment objective: per product sensitivity)	Continuous during storage period
Excursion detection record	Automated alert when any monitored parameter exits the acceptable range	Generated at moment of excursion detection	Real-time
Excursion assessment	Documented evaluation of excursion severity, duration, and impact on product integrity	Generated following excursion event by qualified assessor	Event-driven; must be completed within defined SLA per severity
Storage period summary	Aggregate condition report covering the full storage period for a product at a facility	Generated at CUS_STORAGE_EXIT event	Event-driven at storage exit

Excursion Severity Classification:

Severity	Definition	Default Response	Escalation
Minor	Parameter deviation within defined tolerance band; short duration; no expected impact on product integrity	Log excursion; include in storage period summary; no hold required	No escalation unless recurrent (3+ minor excursions in rolling 30 days)
Moderate	Parameter deviation exceeds tolerance band or duration	Hold-only containment; excursion assessment	Tier 1 review if assessment cannot

Severity	Definition	Default Response	Escalation
	threshold; potential impact on product integrity	required before release	confirm product integrity
Severe	Parameter deviation significantly exceeds specification; extended duration; probable impact on product integrity	Immediate hold; quarantine workflow initiated; Preservation Bundle	Incident escalation; Tier 1 or Tier 2 review depending on product category criticality
Critical	Parameter deviation indicating complete storage failure (e.g., cold-chain break for biologics, light exposure for photosensitive products)	Immediate quarantine; presumptive product integrity failure; Preservation Bundle	Incident response per institutional procedures; potential recall assessment

Transition Logging. Every transition between storage states — entry, exit, excursion detection, excursion resolution, condition parameter changes — generates an ILS record linked to the custody event chain. Storage transitions are cross-referenced with the product's provenance manifest to maintain alignment between custody evidence and provenance evidence.

6.3 Handoff, Receipt, Transfer, Quarantine, Release, and Return Workflows

Each custody transition follows a defined workflow producing evidence artifacts at each step. The workflows below are presented as operational sequences — not as prescriptive institutional procedures, but as evidence-generation patterns that produce the artifacts required for downstream reconciliation and reviewer access.

Handoff/Receipt Workflow (Standard Custody Transfer):

```
Step 1: Transfer initiation
  → Transferring entity generates handoff request with product reference,
    quantity, destination, and transport conditions
  → ILS record: CUS_HANDOFF (initiated)

Step 2: Transport documentation
  → Transport conditions documented (carrier, route, expected duration,
    condition monitoring method)
  → Transport evidence linked to handoff record

Step 3: Receipt and verification
  → Receiving entity verifies: product identity (CPO match), quantity,
    condition, packaging integrity
  → ILS record: CUS_RECEIPT with verification result

Step 4: Reconciliation checkpoint
```

→ Receiving entity's custody records reconciled against transferring entity's handoff records
→ Discrepancies trigger reconciliation break workflow (Section 9.6)

Step 5: Custody chain update
→ Product provenance manifest updated with new custody segment
→ Content-addressed linkage established between preceding and new custody events

Quarantine Workflow:

Step 1: Quarantine trigger
→ Trigger condition identified (recall notification, quality alert, integrity failure, regulatory hold, custody anomaly)
→ ILS record: CUS_QUARANTINE_ENTRY with trigger reference

Step 2: Physical/logical segregation
→ Product physically or logically separated from dispensable inventory
→ Segregation verification evidence generated

Step 3: Investigation
→ Investigation workflow initiated per trigger type
→ Investigation evidence logged as ILS records

Step 4: Determination
→ Investigation concludes with one of:
(a) Release — product returns to ACTIVE state
(b) Continued hold — additional investigation required
(c) Destruction — product removed from supply chain
(d) Return to manufacturer — product returned for assessment
→ Determination record with authority, evidence references, and approval chain

Step 5: Resolution execution
→ Appropriate custody event generated (CUS_QUARANTINE_RELEASE, CUS_DESTRUCTION, CUS_RETURN)
→ Provenance manifest updated; custody chain extended

Return Workflow:

```
Step 1: Return initiation
  → Returning entity documents return reason and product condition
  → ILS record: CUS_RETURN (initiated)

Step 2: Receiving assessment
  → Receiving entity assesses returned product: identity verification,
    condition evaluation, custody history review
  → Assessment record generated

Step 3: Disposition determination
  → Product is either: re-entered into dispensable inventory (if
    assessment confirms integrity), quarantined (if assessment raises
    concerns), or destroyed (if product is no longer suitable)
  → Disposition record with authorization

Step 4: Custody chain update
  → Return event and disposition event added to custody chain
  → Provenance manifest updated
```

6.4 Controlled Dispensation and Release-State Logic

Dispensation is the terminal custody event in the standard product lifecycle — the controlled transfer of a medicine or health product to its intended recipient. Dispensation is operationally final when all prerequisite evidence states are satisfied and the dispensation evidence pack is generated. This section defines the precondition gates that must be verified before dispensation proceeds.

Dispensation Precondition Gate (Conceptual):

Gate	Verification Required	Failure Response
G1: Product Authenticity	Product authenticity state = VERIFIED (Section 3.1)	Dispensation blocked; hold-only containment
G2: Authorization Validity	Prescription/authorization validity state = VALID (Section 3.4); issuer legitimacy state = CONFIRMED (Section 3.3)	Dispensation blocked; escalation to authorization review
G3: Scope Match	Authorization bounds match dispensation parameters (product, quantity, location, purpose, channel) per Section 5.3	Dispensation blocked; scope mismatch break generated
G4: Custody Integrity	Chain-of-custody state = INTACT (Section 3.5); no unresolved custody gaps or compromises	Dispensation blocked; custody gap investigation
G5: Safety Evidence	Proof-of-safety state = SUFFICIENT (Section 3.7); required safety evidence classes present and	Dispensation blocked; safety evidence review

Gate	Verification Required	Failure Response
	current	
G6: No Active Hold	Product recall/quarantine/hold state = ACTIVE (Section 3.8); no hold, quarantine, or recall in effect	Dispensation blocked until hold resolved
G7: Revocation Check (Optional)	Where Baseline D patterns applied: authorization and product-reference revocation checks passed within freshness window	Dispensation blocked; re-verification required

Gate Execution Logic. All gates must pass before dispensation proceeds. Gates are evaluated in sequence; a failure at any gate halts the dispensation and triggers the specified failure response. Gate results are logged as part of the dispensation evidence record.

Dispensation Evidence Record. Upon successful gate completion and dispensation execution, a dispensation evidence record is generated containing: all gate verification results with timestamps, the dispensing entity's credential reference, the recipient reference (pseudonymized per institutional privacy policy), the product CPO reference, the authorization reference, the content-addressed linkage to the preceding custody event, and the self-referential content hash. This record becomes the terminal event in the product's custody chain for the dispensation pathway.

Partial Dispensation. Where a prescription authorizes multiple units or refills and dispensation occurs in increments, each partial dispensation generates its own evidence record. Quantity accumulation is tracked against the authorization's quantity bound (Section 5.3). When accumulated dispensation quantity reaches the authorization limit, further dispensation under the same authorization is blocked.

6.5 Custody Gaps, Stale Custody Evidence, and Contamination / Substitution Risk Patterns

Custody integrity failures manifest through recognizable patterns. This section catalogs the primary risk patterns and maps each to the appropriate evidence response.

Custody Risk Pattern Catalog:

Risk Pattern	Detection Method	Evidence Indicator	Response
Custody gap — missing handoff	Provenance manifest review reveals event chain discontinuity; hash linkage breaks between events	CUS_HANDOFF expected but absent; hash chain break at expected transition point	Hold-only containment; Tier 1 investigation; UNRESOLVED provenance state
Stale custody evidence — outdated condition records	Continuous condition log shows gap exceeding defined freshness threshold	Last condition reading exceeds staleness limit for product category	Re-assessment required; dispensation blocked until fresh condition evidence obtained
Unauthorized custody event — unrecognized	Custody event record contains actor identifier not in authorized	Actor ID fails credential verification; no AES linkage	Immediate hold; incident escalation; Preservation Bundle;

Risk Pattern	Detection Method	Evidence Indicator	Response
actor	custodian registry		potential COMPROMISED custody state
Storage condition violation — unassessed excursion	Excursion detection record exists without corresponding excursion assessment	CUS_TEMP_EXCURSION logged but no assessment record within SLA	Hold-only containment until excursion assessment completed
Product identity mismatch at receipt	CUS_RECEIPT verification indicates product CPO mismatch with handoff documentation	Product reference in receipt record differs from handoff record	Immediate hold on affected product; reconciliation break; potential counterfeit investigation
Quantity discrepancy at handoff	CUS_RECEIPT quantity does not match CUS_HANDOFF quantity	Quantity fields diverge between sender and receiver records	Reconciliation break; investigation per severity (minor variance vs. significant discrepancy)
Repackaging without authorization	CUS_REPACKAGE event lacks authorized repackager credential	Repackaging entity AES absent or unverified	Hold-only containment on repackaged units; Tier 1 investigation of repackager authority

Contamination and Substitution Indicators. While the framework does not perform laboratory analysis or physical inspection, certain evidence patterns indicate elevated contamination or substitution risk requiring institutional investigation: multiple products in the same custody chain with overlapping storage periods and incompatible storage requirements; product identity verification failures at multiple custody nodes in the same supply chain segment; custody gaps coinciding with known diversion or counterfeit activity patterns; and repackaging events by entities without documented repackaging authority.

6.6 Custody Replay for Disputes and Review Reconstruction

When a dispute, adverse event, or supervisory inquiry requires reconstruction of a product's custody history, the custody replay capability enables reviewers to traverse the complete custody event chain from any point to any other point.

Replay Procedure (Conceptual):

1. **Scope definition.** Reviewer specifies the product reference (CPO), the time window, and the review purpose (purpose code per Baseline C/D conventions).
2. **Access authorization.** Reviewer access authorized at the appropriate tier (Tier 0 for aggregate custody statistics; Tier 1 for specific product custody chain; Tier 2 for underlying entity identities). TTL assigned. Access event logged.

3. **Chain retrieval.** Custody Evidence Set (CES) retrieved from content-addressed storage. Hash chain integrity verified — if any event record has been tampered with, the hash verification fails and an integrity alert is generated.
4. **Timeline reconstruction.** Custody events are assembled in chronological order, cross-referenced against the provenance manifest, and presented as a reviewable timeline. Each event includes the acting entity (pseudonymized at Tier 1; identified at Tier 2), the product reference, the event type, conditions, and evidence references.
5. **Gap identification.** Any custody gaps — periods where the product's custodial responsibility is undocumented — are flagged with the gap's duration, the last known custodian, and the next documented custodian.
6. **Post-access review.** Reviewer's access scope, findings, and any follow-up actions are documented in the Post-Access Review Pack per Baseline C/D conventions.

Dispute-Specific Replay. In custody disputes between parties (e.g., distributor and pharmacy disagreeing about product condition at handoff), the replay capability provides both parties' custody event records for the disputed transition. Discrepancies are classified as reconciliation breaks (Section 9.6) and resolved through the dispute-handling framework (Section 8.6).

6.7 Offboarding or Recall-State Custody Continuity

When a product is subject to offboarding (transition to a legacy tracking system) or a recall, custody continuity must be maintained through the transition to ensure that the product's full custody history remains reconstructable.

Recall-State Custody Continuity Requirements:

- When a recall is initiated (Section 8.2), all custody holders of affected products must acknowledge the recall (CUS_RECALL_ACK) and report their affected inventory.
- Products subject to recall remain in the custody chain — the recall does not erase or overwrite prior custody events. The recall generates additional custody events (acknowledgment, quarantine, return, or destruction) that extend the chain.
- Recall scope determination uses the aggregation hierarchy (Section 4.5) to identify all downstream units affected by a batch/lot-level recall. The custody chain for each affected unit is traversed to identify current custodians.
- Recall closure requires evidence that all affected units have been accounted for — returned, destroyed, quarantined, or otherwise resolved — with reconciliation between the recall scope determination and the cumulative custody event responses.

Offboarding Custody Continuity Requirements:

- When a product's tracking transitions from the framework's evidence system to a legacy system, an offboarding proof bundle is generated per Baseline A (Section 12) conventions.
- The offboarding proof bundle includes the complete custody event chain for the product, the provenance manifest, all content-addressed integrity markers, and a final reconciliation checkpoint.

- The legacy system's ingestion of custody records is verified, and acceptance evidence is generated confirming that the legacy system accurately reflects the product's custody history at the point of transition.
- Post-offboarding, the framework's copy of the custody evidence is archived with retention policies consistent with applicable institutional requirements (alignment objective: typically 7+ years).

---

7. Proof-of-Safety and Context-Bound Clinical Decision Evidence

7.1 Proof-of-Safety as Operational Evidence, Not a Legal or Medical Conclusion

This framework treats proof-of-safety as an operational evidence condition — a documented state indicating that specified categories of safety-relevant evidence exist, are current, and are internally consistent for a given product, dispensation, or clinical decision. Proof-of-safety is not a determination that a product is safe, that a clinical decision is correct, or that a treatment is appropriate.

What Proof-of-Safety Evidence Demonstrates:

- That defined evidence classes were consulted, recorded, and preserved.
- That the evidence was current (within applicable freshness windows) at the time of the decision or release.
- That no unresolved conflicts exist between evidence classes (e.g., a contraindication flag and a release decision coexisting without resolution documentation).
- That the evidence context can be independently reconstructed by a reviewer without requiring access to the originating clinical system.

What Proof-of-Safety Evidence Does Not Demonstrate:

- That the product is safe in any absolute sense.
- That the clinical decision was medically correct.
- That the treatment will produce a favorable outcome.
- That the prescriber, pharmacist, or clinician exercised appropriate judgment.

These latter determinations remain the province of licensed practitioners, institutional review processes, quality systems, and competent regulatory authorities. The framework provides the evidence substrate that supports, documents, and preserves those determinations for independent review — it does not make the determinations.

7.2 Evidence Classes Supporting Proof-of-Safety

Proof-of-safety state is determined by the presence, currency, and internal consistency of defined evidence classes. The evidence classes are organized into two categories: product-level evidence (pertaining to the medicine or health product itself) and decision-level evidence (pertaining to a specific clinical decision, dispensation, or release).

Product-Level Evidence Classes:

Evidence Class	Description	Freshness Requirement	Source
PS-01: Product safety profile reference	Pointer to the product's current safety information (alignment objective: approved labeling, product monograph, or equivalent)	Verified at product onboarding; re-verified at material change or recertification	Manufacturer or authoritative product registry
PS-02: Known adverse reaction profile	Reference to the product's documented adverse reaction profile at the time of the relevant action	Updated per institutional governance cadence or upon manufacturer safety update	Manufacturer safety communications; institutional formulary systems
PS-03: Storage condition compliance	Evidence that product was stored within specified conditions throughout custody chain (Section 6.2)	Continuous during storage; summarized at each custody transition	Storage condition monitoring systems
PS-04: Product integrity confirmation	Evidence that product's physical integrity (packaging, labeling, appearance) is consistent with specifications	At receipt and at dispensation	Custody event records (CUS_RECEIPT, CUS_DISPENSATION)
PS-05: Recall/withdrawal status	Confirmation that product is not subject to active recall, withdrawal, or safety hold	Verified at dispensation; freshness per reconciliation cadence	Recall status registry or institutional safety alert system

Decision-Level Evidence Classes:

Evidence Class	Description	Freshness Requirement	Source
DS-01: Contraindication screening output	Record of contraindication assessment for the specific patient-product combination	Generated at or before dispensation; current to formulary version at time of assessment	Clinical decision-support system or pharmacist review
DS-02: Drug interaction screening output	Record of drug interaction assessment against the patient's known medication profile	Generated at or before dispensation; current to interaction database version at assessment time	Clinical decision-support system or pharmacist review
DS-03: Dosage/quantity appropriateness record	Record of dosage or quantity verification against product specifications and authorization parameters	Generated at dispensation; validated against authorization bounds	Dispensing system or pharmacist verification
DS-04: Clinical decision-support output (high-impact)	Record of algorithmic or decision-support system output for high-impact clinical decisions (Section 7.3)	Generated at decision time; version-stamped to algorithm/database version	Clinical decision-support system

Evidence Class	Description	Freshness Requirement	Source
DS-05: Prescriber clinical rationale (where applicable)	Documented prescriber rationale for decisions outside standard parameters (off-label use, dose escalation, therapeutic substitution)	Generated at authorization; preserved for review	Prescriber documentation system

Minimum Evidence Requirements by Action Type:

Action Type	Required Product-Level Classes	Required Decision-Level Classes
Standard dispensation	PS-01, PS-03, PS-04, PS-05	DS-01, DS-02, DS-03
High-impact dispensation (narrow therapeutic index, biologics, controlled substances)	PS-01, PS-02, PS-03, PS-04, PS-05	DS-01, DS-02, DS-03, DS-04
Off-label or non-standard dispensation	PS-01, PS-02, PS-03, PS-04, PS-05	DS-01, DS-02, DS-03, DS-05
Clinical decision review (post-hoc)	PS-01, PS-02	DS-01, DS-02, DS-04 (where applicable)

7.3 Context-Bound Decision States and Reviewer-Safe Outputs

High-impact clinical decisions — dose calculations for narrow therapeutic index products, contraindication overrides, formulary exception approvals, treatment protocol selections — generate decision-state evidence that must be preserved in a form enabling independent reviewer reconstruction.

Context-Bound Decision State — Definition. A context-bound decision state records the complete evidence context that existed at the moment a clinical decision was made or a decision-support output was generated. The "context-bound" qualifier distinguishes this from a free-standing decision record: the decision is meaningful only in the context of the evidence state that supported it.

Context-Bound Decision State — Minimum Fields:

Field	Description
decision_id	Unique content-addressed identifier for this decision record
decision_type	Category of decision (dispensation approval, contraindication override, dosage calculation, formulary exception, protocol selection)
decision_timestamp	UTC timestamp of decision execution
decision_actor	Pseudonymized or role-based identifier for the decision-maker (clinician, pharmacist, system)
evidence_snapshot	Content-addressed references to all evidence classes consulted at decision time (PS and DS classes per Section 7.2)
algorithm_version (if applicable)	Version identifier for any decision-support algorithm, formulary database, or interaction database used
input_parameters	Abstracted or categorized input parameters (not raw patient data by

Field	Description
(abstracted)	default — per bounded disclosure principle)
output_result	The decision-support output or decision determination
override_flag	Boolean indicating whether the decision overrides a system-generated alert or recommendation
override_justification (if applicable)	Documented rationale for override, linked to DS-05 evidence class
content_address	Self-referential hash of the complete decision state record

Reviewer-Safe Outputs. The context-bound decision state is designed to be reviewer-safe — meaning a reviewer can independently assess the decision's evidence basis without requiring access to the originating clinical system. The reviewer examines:

- Whether the required evidence classes were present at decision time (completeness check).
- Whether the evidence was current at decision time (freshness check against the evidence snapshot timestamps and the applicable freshness windows).
- Whether the algorithm or database version was current at decision time (version consistency check).
- Whether any override was documented with justification (override accountability check).
- Whether the decision output is consistent with the evidence context as recorded (internal consistency check).

The reviewer does not need access to raw patient data, full clinical records, or the originating system's internal state. The bounded verification principle (Section 3.12) applies: Tier 1 review accesses the decision state record and evidence references under documented purpose code and TTL; Tier 2 review accesses underlying patient or clinician identifiers only under objective triggers with dual-control approval.

7.4 High-Impact Instruction or Decision Review Posture

Not all clinical decisions require the same level of evidence preservation and review capability. The framework applies a graduated review posture based on the potential impact of the decision.

Review Posture Classification:

Review Posture	Applicable Decisions	Evidence Requirement	Preservation
Standard	Routine dispensation with standard safety checks; no alerts triggered; no overrides	Product-level evidence classes (PS-01 through PS-05) and standard decision-level classes (DS-01 through DS-03)	Standard retention per institutional policy
Enhanced	Dispensation of high-risk products (narrow therapeutic index, biologics, controlled substances); decisions involving dose calculations near therapeutic boundaries	All applicable evidence classes including DS-04; context-bound decision state record generated	Extended retention; available for Tier 1 review

Review Posture	Applicable Decisions	Evidence Requirement	Preservation
Exceptional	Override of system-generated safety alert; off-label use; formulary exception; therapeutic substitution; emergency authorization	All applicable evidence classes including DS-04 and DS-05; context-bound decision state with override documentation	Preservation Bundle generated; available for Tier 1 and Tier 2 review; mandatory post-decision review within institutional SLA

Review Posture Determination. The review posture is determined at decision time based on the decision type, the product category, and whether alerts or overrides are involved. The posture classification is recorded as a field in the decision state record and governs the evidence preservation and access requirements.

7.5 Stale Evidence, Superseded Evidence, and Unresolved Safety-State Ambiguity

Safety evidence has a temporal dimension — evidence that was current at the time of a decision may become stale or superseded before downstream actions (additional dispensation, refill, reimbursement) are completed.

Stale Evidence. A safety evidence artifact is stale when the time elapsed since its generation exceeds the applicable freshness window for its evidence class. Stale evidence does not constitute a safety failure per se — it triggers a defined stale-evidence handling workflow:

1. Dispensation or release action blocked pending evidence refresh.
2. Re-verification performed against current databases, formularies, or safety information.
3. If re-verification confirms continued validity: evidence refreshed; action proceeds.
4. If re-verification reveals changed conditions (new contraindication, updated adverse reaction profile, changed formulation): safety evidence state transitions to SUPERSEDED; re-assessment required per Section 7.6.

Superseded Evidence. A safety evidence artifact is superseded when the underlying source data has been materially updated since the artifact's generation. Examples: a product's safety profile is updated with new adverse reaction information; the formulary version referenced by a decision-support output is replaced by a newer version with different recommendations; a contraindication database is updated with new interactions affecting the product in question.

Supersession does not retroactively invalidate prior decisions — decisions made in good faith based on the evidence state current at decision time are preserved as historical evidence. Supersession affects future actions: any new dispensation, refill, or release that would rely on superseded evidence must first refresh the evidence against the current source.

Unresolved Safety-State Ambiguity. The proof-of-safety state becomes DISPUTED (Section 3.7) when conflicting evidence classes coexist without resolution documentation. Examples: a contraindication screening output flagging a potential interaction and a dispensation authorization proceeding without documented override justification; a product safety update indicating new risks and a continued dispensation pattern without institutional re-assessment evidence. Unresolved

ambiguity triggers hold-only containment for future dispensation events and escalation per Section 7.6.

7.6 Escalation Thresholds for Review, Hold, Recall, or Manual Confirmation

When safety evidence conditions fail to meet the requirements for SUFFICIENT proof-of-safety state, the framework provides structured escalation rather than silent progression or categorical rejection.

Safety Evidence Escalation Matrix:

Condition	Severity	Default Response	Escalation Path	Preservation
Required evidence class absent (e.g., DS-01 not generated before dispensation)	High	Dispensation blocked	Tier 1: review of evidence gap; institutional remediation	Evidence gap record preserved
Safety evidence stale beyond freshness window	Moderate	Dispensation blocked pending refresh	Re-verification workflow; Tier 1 if refresh reveals changed conditions	Stale evidence record preserved alongside refreshed evidence
System-generated safety alert overridden without documentation	High	Post-dispensation review triggered; future dispensation held	Tier 1: review of override circumstances; institutional governance notification	Override event preserved as Preservation Bundle
Product safety profile updated after dispensation but before next refill	Moderate	Next refill blocked pending re-assessment	Institutional safety re-assessment per updated profile; Tier 1 if re-assessment identifies patient safety concern	Updated profile and re-assessment evidence preserved
Conflicting evidence classes without resolution	High	Dispensation blocked; DISPUTED safety state	Tier 1: review of conflicting evidence; clinical determination required	Conflict record preserved; resolution documented
Decision-support algorithm version recalled or deprecated	Moderate–High	Decisions relying on deprecated version flagged for review	Institutional assessment of affected decisions; Tier 1 if scope is significant	Algorithm version change record; affected decision inventory
Multiple safety evidence failures for same product across multiple dispensation points	Critical	Product-level hold-only containment	Institutional safety review; potential recall assessment; Tier 2 if systematic failure suspected	Pattern detection evidence; Preservation Bundle for product

Manual Confirmation Pathway. For any safety evidence condition that blocks dispensation but does not indicate an actual safety risk (e.g., a system timeout preventing contraindication check, a database unavailability preventing interaction screening), the framework supports a manual confirmation pathway: a qualified clinician or pharmacist performs the safety assessment manually, documents the manual assessment with evidence class DS-05, and authorizes dispensation with the manual assessment serving as the evidence artifact. Manual confirmations are classified under the "Enhanced" or "Exceptional" review posture (Section 7.4) regardless of the product category.

7.7 Preservation and Replay for Safety-Relevant Decision States

Safety-relevant decision states are preserved for the duration applicable to the institutional retention policy (alignment objective: typically matching or exceeding the product's shelf life, the prescription's validity period, and any applicable regulatory retention requirement).

Preservation Requirements:

Element	Preservation Duration	Storage Requirements
Context-bound decision state records	Per institutional retention policy; alignment objective: minimum 7 years or as required	Content-addressed storage per Baseline C; integrity verification per reconciliation cadence
Evidence class artifacts referenced by decision states	Same as the decision state that references them	Content-addressed storage; cross-reference linkage maintained
Override justification records	Extended retention — at least as long as the longest applicable review or litigation window	Content-addressed storage; flagged for legal-hold readiness
Safety alert records (system-generated)	Same as decision state retention	Content-addressed storage; linked to decision state and override records
Algorithm/database version snapshots	At least one version beyond the referenced version (enabling version comparison)	Version-controlled storage; retrievable by version identifier

Replay Capability. A reviewer conducting post-hoc review of a safety-relevant decision must be able to reconstruct the decision context by retrieving the context-bound decision state record, verifying the content-addressed integrity of all referenced evidence artifacts, confirming the algorithm and database versions referenced, and assessing whether the decision output was consistent with the evidence context. This replay capability is the clinical-decision analog of "ownership timeline replay" from Baseline A and "settlement chain reconstruction" from Baseline E.

---

8. Review, Recall, Quarantine, Correction, and Supersession Workflows

8.1 Hold-Only Containment Logic

Hold-only containment is the framework's default response to evidence uncertainty. Inherited from Baseline A, the principle is that when evidence integrity is uncertain, the operationally sound response is restriction of state changes while preserving all evidence for investigation — not destructive correction, premature release, or categorical rejection.

Hold-Only Containment — Operating Rules:

- Hold prevents dispensation, release, transfer, claim progression, and any other state change for the affected product, authorization, or evidence artifact. It does not prevent investigation, evidence gathering, or reviewer access.
- Hold does not imply fault, violation, or deficiency. It is a precautionary control triggered by evidence conditions, not by determinations of wrongdoing.
- Hold is applied at the narrowest scope that addresses the evidence condition. A custody gap affecting a single product unit does not hold the entire batch unless the gap pattern suggests broader compromise.
- Hold entry and hold release are both logged as ILS records with content-addressed integrity. The hold record includes the trigger condition, the authority imposing the hold, the scope of affected items, and the expected resolution timeline.
- Hold release requires documented resolution evidence, approval from the appropriate authority (governance body, compliance function, or institutional decision-maker), and a post-release verification step confirming that the resolved evidence state supports the release.

Hold Scope Determination:

Trigger Condition	Default Hold Scope	Escalation to Broader Scope
Single product unit — provenance gap	Individual product unit	If gap pattern repeats across units from same source, extend to source-level hold
Authorization validity dispute	Pending dispensation events linked to disputed authorization	If dispute affects multiple authorizations from same issuer, extend to issuer-level review
Safety evidence stale for product category	Individual dispensation event pending evidence refresh	If staleness affects multiple products in same evidence class, extend to evidence-class review
Storage condition excursion (moderate+)	Product units in affected storage location during excursion period	If excursion severity is critical, extend to all products at facility
Custody chain integrity failure (hash break)	Product units in affected chain segment	Incident-level investigation; scope determined by integrity failure analysis
Recall notification received	All product units matching recall scope (batch/lot, product, date range)	Per recall scope as defined by issuing authority

8.2 Recall and Quarantine State Transitions

Product recalls, quarantines, and safety holds follow a defined state transition model with evidence generation at each transition.

Recall State Machine:

```
ACTIVE (normal operational flow)
  → RECALL_INITIATED (recall notification issued)
    → RECALL_ACKNOWLEDGED (custody holders acknowledge; inventory reported)
      → QUARANTINED (affected products segregated)
        → RETURNED (products returned to manufacturer/designated entity)
          → DESTROYED (products destroyed under documented conditions)
          → RE-ASSESSED (products assessed for potential re-release)
            → RELEASED_FROM_RECALL (if re-assessment confirms safety)
            → DESTROYED (if re-assessment confirms deficiency)
      → RECALL_CLOSED (all affected units accounted for)
```

Recall Evidence Requirements at Each Transition:

Transition	Evidence Generated	Accountability
ACTIVE → RECALL_INITIATED	Recall notification record: affected product reference (CPO, batch/lot), recall reason, scope determination, issuing authority, urgency classification	Recall authority (manufacturer, regulatory body, or institutional quality function)
→ RECALL_ACKNOWLEDGED	Acknowledgment record from each downstream custody holder: affected inventory assessment, containment actions taken	Each custody holder
→ QUARANTINED	Quarantine entry records (CUS_QUARANTINE_ENTRY) for all identified units; segregation verification	Custody holders
→ RETURNED or DESTROYED	Return custody chain records or destruction evidence (CUS_DESTRUCTION) with witness documentation	Custody holders and recall authority
→ RECALL_CLOSED	Recall closure report: scope vs. resolution reconciliation (all affected units accounted for); open items documented; closure authorization	Recall authority with governance approval

Quarantine as Independent Action. Quarantine may also be initiated independently of a recall — for example, in response to a custody integrity failure, a quality alert, or a regulatory hold. Independent quarantine follows the same custody event taxonomy (CUS_QUARANTINE_ENTRY, CUS_QUARANTINE_RELEASE) and evidence requirements, but is not linked to a recall scope determination.

8.3 Correction and Reclassification Pathways

Corrections address errors in evidence artifacts — incorrect timestamps, wrong product references, erroneous actor identifiers, miscategorized events — without destroying the original record.

Correction Principles (Inherited from Baseline A):

1. **Non-destructive.** The original record is preserved in its original form. No silent overwrites.
2. **EP Delta generated.** Every correction produces an EP Delta artifact documenting the prior state, the corrected state, the correction reason, and the correction authority.
3. **Supersession chain maintained.** The corrected record becomes the current-reference state; the original record becomes historical preserved state with a pointer to the correction.
4. **Downstream impact assessed.** The correction EP Delta includes an assessment of downstream actions that relied on the original (now-corrected) record. Dependent actions may require re-verification or adjustment.
5. **Approval chain documented.** Corrections require documented authorization — the entity or governance process that approved the correction, the evidence basis for the correction, and the approval timestamp.

Reclassification. Reclassification is a specific type of correction where a product, authorization, or evidence artifact changes category. Examples: a product reclassified from standard dispensation to controlled substance; a prescription reclassified from renewal to new prescription due to changed clinical circumstances; a safety evidence class reclassified from SUFFICIENT to SUPERSEDED following a product safety update. Reclassification follows the same EP Delta and non-destructive preservation discipline as any other correction.

Correction Authority Matrix:

Correction Type	Authorized Corrector	Approval Requirement	Evidence
Factual error in custody event record (wrong timestamp, incorrect quantity)	Operating entity that generated the original record	Dual authorization (originator + supervisor)	Correction EP Delta with error description and supporting evidence
Product reference correction (CPO error, wrong batch/lot linkage)	Manufacturer or authoritative product registry	Governance approval; higher scrutiny due to provenance chain implications	Correction EP Delta; provenance manifest update; downstream re-verification
Authorization correction (scope error, issuer reference error)	Issuing authority or institutional governance	Governance approval; downstream dispensation review if already dispensed	Correction EP Delta; affected dispensation event inventory
Safety evidence correction (incorrect classification, erroneous alert)	Evidence source system operator with clinical/quality review	Clinical or quality review plus governance documentation	Correction EP Delta; affected decision state review
Recall scope correction	Recall authority	Governance	Recall scope correction

Correction Type	Authorized Corrector	Approval Requirement	Evidence
(over-inclusive or under-inclusive initial scope)		documentation; downstream notification of scope change	record; updated notification to custody holders

---

8.4 Supersession Chains and Current-Reference State Determination

When an evidence artifact, authorization, product state, or safety assessment is replaced by a newer version, the framework maintains a supersession chain linking all versions in chronological order.

Supersession Chain Structure:

```
supersession_chain:
  chain_id: [content_address]
  subject_type: AUTHORIZATION | PRODUCT_STATE | SAFETY_EVIDENCE | CPO
  subject_reference: [content_address of subject]
  versions:
    - version_number: 1
      state: SUPERSEDED
      content_address: [hash of version 1]
      created_at: [UTC]
      superseded_at: [UTC]
      superseded_by: [hash of version 2]
    - version_number: 2
      state: SUPERSEDED
      content_address: [hash of version 2]
      created_at: [UTC]
      superseded_at: [UTC]
      superseded_by: [hash of version 3]
    - version_number: 3
      state: CURRENT
      content_address: [hash of version 3]
      created_at: [UTC]
  current_reference: [hash of version 3]
  chain_content_address: [self-referential hash]
```

Current-Reference State Determination Rules:

- The current-reference state is always the most recent version in the supersession chain that has not been revoked.

- If the most recent version has been revoked, the current-reference state is REVOKED — the framework does not automatically fall back to a prior version. Re-authorization or re-assessment is required.
- Downstream actions must bind to the current-reference state. Actions bound to a superseded version generate reconciliation breaks.
- Supersession chain traversal is available to reviewers at the appropriate tier, enabling version history reconstruction.

8.5 Non-Destructive Preservation of Prior States

Every state change — correction, supersession, revocation, recall, reclassification — preserves the prior state in its original, unmodified form. This principle is foundational and non-negotiable within the framework.

Preservation Mechanisms:

Change Type	Prior State Treatment	Retrieval Method
Correction	Original record retained with CORRECTED status; linked to correction EP Delta	Retrieve by original content address; correction EP Delta contains pointer to both versions
Supersession	Prior version retained with SUPERSEDED status; linked via supersession chain	Traverse supersession chain; prior versions accessible by version number or content address
Revocation	Revoked artifact retained with REVOKED status; revocation record linked	Retrieve by content address; revocation record provides context
Recall	Pre-recall product state and custody evidence preserved	Retrieve complete custody chain including pre-recall events; recall events are additive, not overwriting
Hold/release cycle	Pre-hold state, hold record, and post-release state all preserved	Full hold lifecycle available: trigger → hold entry → investigation → resolution → release

Prohibited Actions:

- Deletion of evidence artifacts from content-addressed storage during retention period.
- Modification of content-addressed artifacts after storage (modification creates a new content address, breaking linkage).
- Silent overwrite of any state without generating a correction EP Delta or supersession record.
- Selective purging of historical versions from supersession chains.

Any detected violation of these preservation rules is treated as a governance violation, logged as a liability trigger event per Baseline C conventions, and subject to incident investigation.

8.6 Dispute-Handling and Post-Resolution Review

Disputes arise when parties disagree about the evidence state of a product, authorization, custody record, or safety assessment. The framework provides structured dispute-handling that produces evidence artifacts and preserves all parties' positions.

Dispute Workflow:

```
Step 1: Dispute initiation
  → Disputing party submits dispute record with:
    subject reference, nature of dispute, claimed evidence state,
    supporting documentation
  → ILS record generated; hold-only containment applied to disputed subject

Step 2: Counter-evidence gathering
  → Responding party(ies) submit their evidence artifacts
  → All submissions content-addressed and preserved

Step 3: Reconciliation attempt
  → Framework's reconciliation logic applied to identify specific
    evidence discrepancy
  → Break classification per Section 9.6

Step 4: Determination
  → Determination authority (institutional governance, designated
    arbitrator, or regulatory authority as applicable) reviews
    evidence from all parties
  → Determination record generated with authority, reasoning,
    and evidence references

Step 5: Resolution execution
  → Correction, supersession, or confirmation applied per determination
  → EP Delta generated
  → Hold released with resolution evidence

Step 6: Post-resolution review
  → All dispute evidence, determination records, and resolution
    artifacts compiled into a Preservation Bundle
```

```
→ Post-resolution review conducted to identify process improvements
→ Lessons learned documented per governance framework
```

Dispute Evidence Preservation. All dispute-related evidence — initiation records, counter-evidence submissions, reconciliation analysis, determination records, and resolution artifacts — is preserved as a Preservation Bundle per Baseline C conventions. The bundle is available for Tier 1 reviewer access under documented purpose code and TTL.

8.7 Downstream Propagation and Closure Conditions

When a correction, recall, revocation, or supersession event affects upstream evidence, the framework requires propagation assessment to identify and address downstream actions that relied on the now-changed evidence state.

Downstream Propagation Logic:

Upstream Change	Downstream Actions Affected	Propagation Requirement	Closure Condition
Product recalled (batch/lot level)	All dispensation events for affected batch/lot; all pending claims linked to affected products	Notification to all dispensation points; claim hold for affected products; patient notification per institutional policy	All affected units accounted for (returned, destroyed, or assessed); all affected claims adjusted or resolved
Authorization revoked	All pending dispensation events linked to revoked authorization; all claims referencing revoked authorization	Dispensation hold; claim hold; re-authorization required for continuation	All pending dispensations either re-authorized or cancelled; all claims adjusted
Safety evidence superseded	All future dispensation events for affected product; open prescriptions referencing stale safety evidence	Evidence refresh required before next dispensation; prescriber notification if safety profile materially changed	All affected prescriptions re-assessed; all future dispensation events operating on current evidence
Custody integrity failure detected	All products in affected custody chain segment; all downstream dispensation and claim events	Hold-only containment on affected products; investigation of custody chain; downstream event review	Investigation concluded with determination; affected products re-verified or quarantined; custody chain repaired or documented
Correction to product identity (CPO)	All evidence artifacts referencing corrected CPO	Provenance manifest update; downstream evidence re-linkage to corrected CPO	All evidence artifacts verified against corrected CPO; reconciliation confirms alignment

Closure Documentation. Each propagation event is tracked until closure. Closure requires: confirmation that all affected downstream actions have been identified, notification sent to affected parties, appropriate holds or adjustments applied, and resolution evidence documented. The propagation tracking record, including closure evidence, is preserved as part of the correction, recall, or supersession Preservation Bundle.

Incomplete Propagation. If propagation cannot reach all affected downstream actions within the governance SLA (e.g., a recalled product has been dispensed and the dispensation point cannot locate the recipient), the framework does not treat this as a resolution — it maintains the propagation item as an open break in the open breaks register (adapted from Baseline E, Section 10.2), subject to escalation and continued monitoring.

---

9. Evidence Artifacts, Manifests, Reconciliation, and Preservation

9.1 Evidence Pack Architecture for Authenticity, Provenance, Authorization, Custody, and Proof-of-Safety States

Every operational state defined in Section 3 — product authenticity, provenance, issuer legitimacy, prescription validity, chain-of-custody, dispensation, proof-of-safety, recall/hold, correction/supersession, and optional claim/reimbursement — is backed by a structured evidence pack. Evidence packs follow the architecture established in Baseline C's Evidence Pack Manifest Template, adapted for healthcare state categories.

Evidence Pack Taxonomy for Healthcare States:

Evidence Pack Type	Abbreviation	Contents	Baseline Analog
Product Authenticity Evidence Set	PAES	CPO, manufacturer credential reference, batch/lot release records, provenance manifest, integrity verification results	Ownership Evidence Set (OES) — Baseline A
Authorization Evidence Set	AES	Issuer credential reference, scope attestation, currency check, revocation check result, freshness status	Disclosure Evidence Pack (DEP) — Baseline A
Custody Evidence Set	CES	Custody event chain (all CUS_ events), storage condition logs, handoff confirmations, excursion records	Custody Evidence Pack (CEP) — Baseline B
Safety Evidence Set	SES	Product-level evidence classes (PS-01 through PS-05), decision-level evidence classes (DS-01 through DS-05), context-bound decision state records	Surveillance Evidence Pack (SEP) — Baseline C
Dispensation Evidence Pack	DEP-H	Dispensation precondition gate results, dispensation event record, authorization linkage, recipient reference, product verification	Settlement Evidence Pack — Baseline E
Preservation Bundle	PB	Incident-specific evidence collection: break detection records, investigation logs, resolution evidence, post-review documentation	Preservation Bundle (PB) — Baseline C

Evidence Pack Manifest Structure. Each evidence pack includes a manifest — a content-addressed index of all artifacts within the pack. The manifest follows Baseline C's manifest schema:

```
evidence_pack_manifest:
```

```
pack_id: [content_address]
pack_type: PAES | AES | CES | SES | DEP-H | PB
subject_reference: [CPO content_address or authorization ID or
                    custody chain ID]
generation_timestamp: [UTC]
generating_entity: [pseudonymized or role-based ID]
period_start: [UTC]
period_end: [UTC]
artifact_inventory:
  - artifact_id: [content_address]
    artifact_type: [ILS | EP_Delta | condition_log | credential_ref | ...]
    artifact_timestamp: [UTC]
  - ...
completeness_checklist:
  required_elements_present: [boolean per element]
  gaps_documented: [list of missing elements with reason codes]
integrity_verification:
  method: SHA-256
  manifest_content_address: [self-referential hash]
  chain_verification_result: PASS | FAIL
retention_metadata:
  retention_class: [class identifier]
  retention_period: [alignment objective: 7+ years]
  legal_hold_status: [boolean]
```

Cross-Pack Linkage. Evidence packs do not exist in isolation. A dispensation evidence pack (DEP-H) references the PAES for the dispensed product, the AES for the authorizing prescription, the CES for the custody chain, and the SES for the safety evidence. These cross-references are maintained through content-addressed pointers — each pack's manifest contains the content addresses of the related packs. A reviewer can traverse from any evidence pack to all related packs by following the content-addressed references.

9.2 Minimum Logging Taxonomy

All operational events within the framework are logged using a standardized event taxonomy aligned with Baseline C's minimum logging taxonomy. Healthcare-specific event categories extend the baseline taxonomy without modifying it.

Healthcare Event Categories (Extending Baseline C):

Event Category	Event Types	Description
Product events	PRODUCT_REGISTERED, PRODUCT_VERIFIED, PRODUCT_FAILED, PRODUCT_RECALLED, PRODUCT_WITHDRAWN	Product lifecycle events from CPO registration through recall or withdrawal
Authorization events	AUTH_ISSUED, AUTH_RENEWED, AUTH_EXPIRED, AUTH_REVOKED, AUTH_SUSPENDED, AUTH_SUPERSEDED	Prescription and authorization lifecycle events
Custody events	CUS_RECEIPT, CUS_HANDOFF, CUS_STORAGE_ENTRY, CUS_STORAGE_EXIT, CUS_TEMP_EXCURSION, CUS_REPACKAGE, CUS_QUARANTINE_ENTRY, CUS_QUARANTINE_RELEASE, CUS_DISPENSATION, CUS_RETURN, CUS_DESTRUCTION, CUS_RECALL_ACK, CUS_HOLD_ENTRY, CUS_HOLD_RELEASE	Full custody event taxonomy per Section 6.1
Safety evidence events	SAFETY_ASSESSED, SAFETY_SUPERSEDED, SAFETY_ALERT_GENERATED, SAFETY_ALERT_OVERRIDDEN, SAFETY_EVIDENCE_REFRESHED	Safety evidence lifecycle events per Section 7
Reconciliation events	RECON_EXECUTED, RECON_BREAK_DETECTED, RECON_BREAK_RESOLVED, RECON_ALIGNED	Reconciliation execution and break lifecycle
Reviewer access events	TIER0_ACCESS, TIER1_ACCESS, TIER2_ACCESS, ACCESS_EXPIRED, POST_ACCESS_REVIEW	Tiered reviewer access events per Section 10
Governance events	GOVERNANCE_APPROVAL, CHANGE_CONTROL, RECERT_TRIGGERED, MATERIAL_CHANGE, LIABILITY_TRIGGER	Governance lifecycle events per Section 11

Minimum Event Attributes. Every logged event must include the fields specified in Baseline C's logging schema: unique event identifier, UTC timestamp (millisecond precision, authoritative time source), event type from the taxonomy above, actor identifier (pseudonymized or role-based), affected resource identifier (product CPO, authorization ID, custody chain reference), event outcome (success, failure, pending), severity (info, low, medium, high, critical), integrity hash (content address of this event record), previous event hash (for hash chain continuity), redaction flag (boolean indicating PII minimization applied), and retention class.

9.3 Content-Addressed Manifest Patterns

All evidence artifacts — ILS records, evidence pack manifests, EP Deltas, provenance manifests, condition logs, decision state records — are stored using content-addressed storage per Baseline C conventions. Content addressing means that each artifact is stored and retrieved using the cryptographic hash of its content as the identifier.

Content-Addressing Operating Rules:

1. **Immutability by construction.** A content-addressed artifact cannot be modified after storage without generating a new content address — which would break all references to the original artifact.
2. **Tamper detection by verification.** To verify an artifact's integrity, a reviewer computes its content hash and compares it to the stored content address. A mismatch indicates tampering or corruption.
3. **Deduplication.** Identical artifacts produce identical content addresses, enabling efficient storage.
4. **Linkage integrity.** Evidence packs reference artifacts by content address. If an artifact is replaced (correction, supersession), the reference in the evidence pack manifest changes — and the change itself is logged as an EP Delta.

Manifest Patterns for Healthcare Evidence:

Manifest Type	Contents Indexed	Update Trigger	Integrity Check
Provenance manifest	All provenance events for a product unit/aggregation	Each custody transition event	Hash chain verification across all events
Authorization manifest	All authorization lifecycle events for a prescription	Each authorization state change	Hash chain verification; supersession chain integrity
Custody manifest	All custody events for a product unit	Each custody event	Hash chain verification; cross-reference to provenance manifest
Safety evidence manifest	All safety evidence artifacts for a product-decision combination	Each safety evidence generation or supersession	Content-address verification of all referenced evidence classes
Reconciliation manifest	All reconciliation execution records and break reports for a defined scope	Each reconciliation execution	Hash chain across reconciliation cycles; break resolution linkage

---

9.4 Chain-of-Custody for Product Evidence and Decision-State Evidence

Evidence artifacts themselves — not only physical products — require chain-of-custody documentation. The chain-of-custody for evidence artifacts documents every access, modification, transfer, and submission event from artifact creation through final archival.

Evidence Chain-of-Custody — Required Fields Per Event:

Field	Description
action_type	creation, access, review, export, transfer, submission, archival
timestamp	UTC timestamp with millisecond precision
actor_id	Pseudonymized or role-based identifier of the entity performing the action
location	System, facility, or storage layer where the action occurred
justification	Purpose code per Baseline C/D conventions; documented reason for the action
verification	Content-address verification result at time of action (confirms artifact integrity)

Evidence Chain-of-Custody vs. Product Chain-of-Custody. The framework maintains two parallel chains: the product custody chain (Section 6) documenting the physical product's custodial journey, and the evidence custody chain documenting the evidence artifacts' access and handling

history. Both chains are content-addressed and hash-chained. The evidence custody chain is essential for examiner confidence: a reviewer must be able to confirm that the evidence artifacts presented during a review have not been altered since their creation.

9.5 Reconciliation Cadence Design

Reconciliation is the continuous or periodic process of verifying alignment between related evidence states — provenance records and custody records, authorization records and dispensation records, safety evidence and current safety data sources, and claim records and underlying dispensation evidence. Reconciliation cadences are calibrated to the volatility and criticality of the evidence states being reconciled.

Reconciliation Cadence Matrix:

Reconciliation Type	Scope	Default Cadence	Event-Driven Triggers
Provenance-Custody Alignment	Provenance manifest vs. custody event chain for each product	Continuous (real-time alerts for critical breaks); daily batch for comprehensive check	Every custody transition event (CUS_HANDOFF, CUS_RECEIPT, CUS_REPACKAGE)
Authorization-Dispensation Alignment	Authorization validity state vs. dispensation events referencing the authorization	At each dispensation event; daily batch for open prescriptions	Dispensation event; authorization state change (renewal, revocation, supersession)
Safety Evidence Currency	Safety evidence classes vs. current source data versions (formulary, interaction database, product safety profile)	Per institutional governance cadence (alignment objective: at least daily for high-risk categories)	Source data update notification; product safety communication; formulary change
Claim-Evidence Alignment (Optional)	Claim/reimbursement records vs. underlying dispensation, authorization, and product evidence	At claim submission; at adjudication; periodic audit cycle	Claim submission; upstream evidence correction or revocation
Aggregate Holdings Reconciliation	Total product units in custody chain vs. manufacturer release records and recall scope determinations	Weekly batch; event-driven for recalls	Recall notification; manufacturer production correction; aggregate discrepancy alert
Offboarding Reconciliation	Framework evidence vs. legacy system records at transition point	At offboarding initiation; at offboarding completion; post-offboarding	Offboarding trigger event

Reconciliation Type	Scope	Default Cadence	Event-Driven Triggers
		verification	

Reconciliation Execution Record. Each reconciliation execution generates a content-addressed report containing: the reconciliation type and scope, the data sources compared, the execution timestamp, the result (ALIGNED or BREAK_DETECTED with break details), and a hash pointer to the previous reconciliation report for the same scope (forming a reconciliation chain).

9.6 Break Taxonomy and Severity Bands

A reconciliation break is a detected mismatch between evidence states that should be aligned. Breaks are classified by type (what kind of mismatch) and severity (operational impact and required response).

Break Type Taxonomy:

Break Type	Description	Example
BRK-PROV	Provenance break — mismatch between provenance manifest and custody records	Custody chain shows handoff to Entity B, but provenance manifest has no corresponding event
BRK-AUTH	Authorization break — mismatch between authorization state and dispensation or claim records	Dispensation references an authorization that has transitioned to EXPIRED or REVOKED
BRK-CUST	Custody break — mismatch between custody records and expected custody state	Product unit recorded at Facility A but receipt record shows Facility B without intervening handoff
BRK-SAFE	Safety evidence break — mismatch between required safety evidence and available evidence	Required evidence class DS-01 (contraindication screening) absent for a completed dispensation
BRK-CLAIM	Claim break — mismatch between claim/reimbursement records and underlying dispensation or authorization evidence	Claim references a dispensation event whose authorization has been subsequently revoked
BRK-INTEG	Integrity break — content-address verification failure for any evidence artifact	Hash of retrieved artifact does not match the stored content address
BRK-FRESH	Freshness break — evidence artifact exceeds applicable freshness window	Issuer legitimacy check performed 45 days ago; freshness window for authority type is 30 days

Severity Bands:

Severity	Definition	Default Response	Resolution SLA
SEV-1: Critical	Break indicates potential safety risk, counterfeit, unauthorized access, or integrity compromise	Immediate hold-only containment; incident escalation; Preservation Bundle	Resolution within 4 hours (containment); full investigation within 48 hours
SEV-2: High	Break indicates material evidence gap or stale evidence that could affect dispensation, claim, or review decisions	Hold-only containment on affected downstream actions; Tier 1 investigation	Resolution within 24 hours

Severity	Definition	Default Response	Resolution SLA
SEV-3: Moderate	Break indicates evidence inconsistency that does not directly affect current safety or dispensation but requires correction	Investigation initiated; no hold unless escalation conditions met	Resolution within 5 business days
SEV-4: Low	Break indicates minor discrepancy (rounding, timestamp precision, non-material metadata)	Logged for correction during next reconciliation cycle	Resolution within 30 days

Break Lifecycle. Each break follows a defined lifecycle: DETECTED → INVESTIGATED → CONTAINED (if applicable) → RESOLVED → CLOSED. Each transition generates an ILS record. A break is CLOSED only when the resolution evidence has been verified and the reconciliation re-execution confirms alignment.

9.7 Preservation Bundles and Legal-Hold-Ready Records

Preservation bundles are comprehensive evidence collections assembled for incidents, disputes, recalls, investigations, or legal hold requirements. The preservation bundle concept is inherited from Baseline C without modification.

Preservation Bundle Trigger Events:

Trigger	Bundle Scope	Mandatory Contents
SEV-1 or SEV-2 reconciliation break	All evidence related to the break: affected product, authorization, custody, and safety evidence	Break detection record, investigation logs, containment evidence, resolution documentation, post-review record
Product recall	All evidence for recalled product batch/lot across all custody holders	Recall notification, scope determination, acknowledgment records, quarantine/return/destruction evidence, closure report
Safety incident or adverse event report	All evidence for the product, authorization, dispensation, and safety assessment involved	Product PAES, authorization AES, custody CES, safety SES, dispensation DEP-H, decision state records
Tier 2 reviewer access event	All evidence accessed during Tier 2 investigation plus the access control records	Tier 2 access request, approval records, accessed evidence inventory, findings, post-access review
Dispute between parties	All evidence submitted by all parties plus reconciliation analysis and determination records	Dispute initiation record, counter-evidence, reconciliation analysis, determination, resolution EP Delta
Legal hold instruction	All evidence within the scope of the legal hold instruction	Scope determination, hold activation record, affected evidence inventory, hold monitoring records
Offboarding event	Complete evidence set for transitioning product, authorization, or custody scope	Final reconciliation, evidence snapshots, legacy transition manifest, ingestion verification

Legal-Hold Readiness. All evidence artifacts are stored in a state that supports legal hold activation without data migration or format conversion. Legal hold activation adds a hold flag to the retention

metadata of affected artifacts, preventing destruction even if the standard retention period expires. Legal hold is removed only upon documented release authorization from the authority that initiated the hold.

9.8 Retrieval and Production Workflows

Evidence retrieval follows the tiered access model (Section 10) with purpose limitation, TTL constraints, and post-access review. Evidence production workflows convert stored evidence artifacts into examination-ready output packages.

Retrieval Service Level Objectives (Alignment Objectives):

Request Type	Target Response Time	Format
Standard examiner query (single product, single state category)	Within 48 hours	Evidence pack with manifest, targeted artifacts, integrity verification
Comprehensive review (multiple products, cross-state-category)	Within 5 business days	Complete evidence pack with cross-referencing, reconciliation history, break inventory
Emergency retrieval (safety incident, active recall, regulatory demand)	Within 4 hours	Priority evidence extraction with integrity verification; completeness may be validated post-delivery
Dispute-related production	Within 48 hours per party's evidence	Structured evidence per dispute-handling framework (Section 8.6)

Production Process:

1. **Request intake.** Purpose code assigned; TTL determined; access tier confirmed.
2. **Scope determination.** Evidence artifacts within the request scope identified through manifest queries and content-addressed retrieval.
3. **Integrity verification.** All retrieved artifacts verified against stored content addresses; any integrity failures flagged.
4. **Minimization and redaction.** Per Baseline C's redaction protocol: PII minimized; prohibited data elements redacted; pseudonymization applied where Tier 1 access; full identifiers included only for Tier 2 access.
5. **Assembly.** Evidence artifacts assembled into the evidence pack folder structure per Baseline C's standard folder structure, with manifest, checksums, and chain-of-custody documentation.
6. **Attestation.** Responsible officer attests to completeness and accuracy of the production.
7. **Delivery.** Pack transmitted through secure channels with delivery confirmation logged.
8. **Post-production documentation.** Production event logged as ILS; access recorded in evidence chain-of-custody.

9.9 Examiner / Reviewer Replay Requirements

Reviewers must be able to reconstruct the operational state of any product, authorization, custody chain, dispensation event, or safety assessment at any historical point. This replay capability is the healthcare analog of "ownership timeline replay" from Baseline A and "settlement chain reconstruction" from Baseline E.

Replay Capability Requirements:

Replay Type	Input	Output	Evidence Traversal
Product authenticity replay	Product CPO reference + target timestamp	Authenticity state at target timestamp with supporting evidence	PAES → provenance manifest → custody chain at timestamp
Authorization timeline replay	Authorization ID + time range	Complete authorization lifecycle within time range	AES → all EP Deltas → supersession chain → dependent dispensation events
Custody chain replay	Product reference + time range	Complete custody event chain within time range with condition records	CES → ordered custody events → storage condition logs → excursion records
Dispensation reconstruction	Dispensation event ID	Complete dispensation evidence: all gate results, authorization linkage, product verification, safety evidence	DEP-H → PAES + AES + CES + SES cross-references
Safety decision replay	Decision state ID	Context-bound decision state with all referenced evidence classes, algorithm versions, and input parameters	SES → decision state record → evidence class artifacts → algorithm version snapshots
Recall scope replay	Recall ID	Complete recall lifecycle: scope determination, downstream propagation, acknowledgment tracking, closure	Recall PB → affected product inventory → custody holder responses → resolution records

---

9.10 Evidence Integrity Failure and Recovery Posture

When evidence integrity checks fail — a content-addressed artifact's hash does not match, a hash chain break is detected, or an artifact is unavailable in storage — the framework treats the failure as a governance incident requiring investigation and recovery.

Evidence Integrity Failure Response:

```
Step 1: Detection and containment
  → Integrity failure detected through hash verification or retrieval failure
  → Affected evidence artifacts flagged; dependent operational states
    placed under hold-only containment
  → ILS record: BRK-INTEG with severity assessment
```

```
Step 2: Investigation
  → Root cause analysis: data corruption, unauthorized modification,
    storage failure, replication lag, or deliberate tampering
  → Investigation logged as ILS records

Step 3: Recovery
  → Valid version restored from replicated storage or backup
  → Restored artifact integrity verified
  → If no valid version exists: evidence gap documented;
    affected operational states re-assessed based on remaining evidence

Step 4: Post-incident review
  → Preservation Bundle generated capturing failure evidence and
    recovery documentation
  → Governance review of integrity controls; recertification trigger
    evaluation per Section 11.4
  → Lessons learned documented
```

Unrecoverable Evidence Loss. If an evidence artifact cannot be recovered from any storage replica or backup, the loss is documented as a permanent evidence gap. Operational states that relied on the lost artifact are re-assessed using remaining evidence. If remaining evidence is insufficient to sustain the operational state (e.g., a VERIFIED authenticity state depends on a lost provenance manifest), the state transitions to UNRESOLVED and hold-only containment applies.

---

10. Tiered Reviewer, Institutional, and Examiner Access

10.1 Tier Definitions

The tiered access model is inherited from Baselines B, C, and D without modification to the tier structure. This section applies the three-tier model to healthcare evidence categories.

Tier 0 — Aggregate / Statistical Access (Default):

Produces aggregate statistics, compliance rates, coverage percentages, and market-level summaries without identifying specific products, prescriptions, patients, or practitioners. Tier 0 is the default access level for all reviewer interactions.

Healthcare Tier 0 outputs include: product authenticity verification pass rates across a participant population, authorization validity check compliance percentages, custody chain integrity rates, dispensation precondition gate pass/fail distributions, safety evidence coverage statistics, reconciliation break counts by type and severity, and recall response completion percentages.

Tier 0 explicitly excludes: individual product provenance details, specific prescription or authorization records, patient-identifiable dispensation records, practitioner-identifiable authorization records, and individual clinical decision state records.

Tier 1 — Scoped / Event-Triggered Access:

Produces scoped evidence extracts for specific products, authorizations, custody chains, or dispensation events under documented purpose codes and TTL constraints. Tier 1 is triggered by specific events (reconciliation breaks, safety alerts, recall investigations, examination requests) and provides pseudonymized references rather than full identity details.

Healthcare Tier 1 outputs include: product provenance manifests for identified products (referenced by CPO, not by patient), authorization lifecycle records for identified prescriptions (referenced by authorization ID, not by patient or prescriber name), custody event chains for identified products, safety evidence artifacts for identified decisions (with practitioner and patient pseudonymized), and reconciliation break investigation records.

Tier 2 — Exceptional Reveal:

Access to underlying identity details — prescriber identity, patient identity, manufacturer identity, specific institutional arrangements — under objective triggers, dual-control approval, strict TTL (default 48-hour initial window), and mandatory post-access review. Tier 2 is reserved for circumstances where Tier 1 evidence is insufficient to resolve the investigation.

Healthcare Tier 2 triggers include: confirmed or suspected counterfeit product detection, practitioner authority fraud investigation, patient safety incident requiring full identity for notification, regulatory enforcement action, and legal hold or litigation discovery requiring full record access.

10.2 Purpose Limitation and TTL

Every reviewer access event — at any tier — operates under purpose limitation and TTL constraints inherited from Baselines C and D.

Purpose Limitation. Each access request specifies a purpose code drawn from a defined purpose code registry. Evidence accessed under a purpose code may not be used for functions outside that code without a new access request and approval cycle.

Healthcare Purpose Code Registry (Illustrative):

Purpose Code	Description	Typical Tier	Default TTL
PUR-EXAM-ROUTINE	Routine examination or audit of operational controls	Tier 0, Tier 1	30 days
PUR-RECON-BREAK	Investigation of specific reconciliation break	Tier 1	14 days
PUR-SAFETY-INCIDENT	Investigation of safety incident or adverse event	Tier 1, Tier 2	30 days
PUR-RECALL-SCOPE	Recall scope determination and	Tier 1	Duration of recall

Purpose Code	Description	Typical Tier	Default TTL
	tracking		lifecycle
PUR-DISPUTE	Dispute investigation between parties	Tier 1	Duration of dispute lifecycle
PUR-ENFORCEMENT	Regulatory enforcement investigation	Tier 1, Tier 2	Per regulatory authority determination
PUR-LEGAL-HOLD	Legal hold or litigation discovery	Tier 1, Tier 2	Duration of legal hold
PUR-COUNTERFEIT	Counterfeit investigation	Tier 1, Tier 2	90 days (renewable)

TTL Operating Rules. Access privileges expire automatically at TTL termination. Expired access cannot be renewed by extending the original grant; a new access request with updated justification is required. TTL expiration events are logged. Evidence accessed during the TTL window remains available for the purpose of documenting findings; the TTL constrains ongoing access, not the use of findings already obtained.

10.3 Default Reviewer-Safe Outputs

By default, all reviewer queries produce reviewer-safe outputs — evidence extracts that provide sufficient information for the review purpose without exposing unnecessary detail. The reviewer-safe output concept is inherited from Baseline D's Verifier Output Pack (VOP) conventions.

Reviewer-Safe Output Principles:

- Product evidence: Reviewer receives product category, batch/lot reference, authenticity state, provenance chain status, and custody chain status. Raw manufacturer commercial details, pricing, and supply chain partner identities are excluded unless Tier 2 access is authorized.
- Authorization evidence: Reviewer receives authorization type, scope, validity state, and issuer legitimacy state. Prescriber name, license number, and practice address are pseudonymized at Tier 1 and revealed only at Tier 2.
- Dispensation evidence: Reviewer receives dispensation event metadata, gate results, and product/authorization linkage. Patient identity is excluded at Tier 0 and Tier 1; pseudonymized at Tier 1 when event-specific investigation requires it; revealed only at Tier 2 under objective triggers.
- Safety evidence: Reviewer receives evidence class presence/absence, freshness status, and override flags. Clinical decision inputs (patient parameters, clinical notes) are abstracted at Tier 1 and accessible only at Tier 2.

10.4 Elevated Access Conditions

Tier 1 access is granted when a documented trigger event justifies scoped access beyond Tier 0 aggregate outputs. Tier 2 access requires additional safeguards.

Tier 1 Elevation Requirements:

Requirement	Detail
Documented trigger	Specific event justifying access (break detection, safety alert, recall, examination request) referenced by event ID
Purpose code	Selected from the purpose code registry; constrains downstream use of accessed evidence
Scope definition	Specific products, authorizations, time windows, or custody chains included; no open-ended scope
TTL assignment	Maximum access duration assigned; auto-expiry enforced
Requesting authority	Identity and institutional affiliation of the requesting reviewer documented
Approval	Single-approval pathway (supervisor or designated access approver)

Tier 2 Elevation Requirements (All Tier 1 Requirements Plus):

Requirement	Detail
Objective trigger	Trigger must meet predefined objective criteria (e.g., confirmed counterfeit indicator, patient safety notification requirement, enforcement referral) — not subjective assessment
Dual-control approval	Two independent approvers required; neither may be the requesting reviewer
Strict TTL	Default 48-hour initial window; renewable in 48-hour increments with documented re-justification
Scope minimization	Access limited to the minimum evidence necessary to address the objective trigger
Post-access review commitment	Mandatory post-access review within defined SLA (default: 5 business days after access termination)
Participant notification plan	Plan for notifying affected parties after investigation, unless notification would compromise ongoing enforcement

---

10.5 Emergency / Dispute Escalation Access

Emergency access addresses situations requiring immediate evidence access to protect patient safety, contain active counterfeit threats, or respond to regulatory emergencies.

Emergency Access Procedure:

1. **Emergency declaration.** Declaring authority identifies the emergency condition and documents the nature of the threat.
2. **Expedited Tier 2 approval.** Dual-control approval obtained on an expedited basis (target: within 2 hours). If one approver is unavailable, a designated alternate approver substitutes with documented justification.
3. **Immediate access granted.** Access activated with strict TTL (24-hour initial window for emergencies; renewable).
4. **Concurrent documentation.** Full access request documentation completed within 24 hours of access activation (post-hoc documentation is permitted for genuine emergencies, not for convenience).
5. **Post-access review.** Mandatory post-access review initiated within 48 hours of access termination; completed within 5 business days.

Dispute Escalation Access. When a dispute between parties (Section 8.6) cannot be resolved at Tier 1, the determination authority may escalate to Tier 2 to access identity-level evidence. Dispute-related Tier 2 access follows standard Tier 2 requirements with the additional constraint that both disputing parties are notified of the escalation.

10.6 Post-Access Review

Every Tier 2 access event and selected Tier 1 access events (per institutional governance policy) require a formal post-access review. The post-access review is inherited from Baselines C and D and constitutes a mandatory accountability control.

Post-Access Review Pack (PARP) — Required Contents:

Element	Description
Access event reference	Event ID of the Tier 1 or Tier 2 access event being reviewed
Reviewer identity	Identity of the post-access reviewer (must be independent of the original accessing reviewer)
Access scope verification	Confirmation that the accessing reviewer stayed within the approved scope; documentation of any scope deviations
Findings summary	Summary of what was found during the access period; findings that support or do not support the initial trigger justification
Data handling confirmation	Confirmation that accessed evidence was handled per minimization, confidentiality, and purpose limitation requirements
Follow-up actions	Any follow-up actions required (additional investigation, referral, remediation, participant notification)
Participant notification status	Whether affected parties were notified; if not, documented justification for deferred notification
Review timestamp	UTC timestamp of review completion
PARP content address	Self-referential hash for tamper-evident preservation

Post-Access Review SLA. Post-access review must be completed within 5 business days of access termination. Overdue reviews generate compliance alerts per the governance escalation framework (Section 11.7). Incomplete post-access reviews are treated as governance violations and logged as liability trigger events.

10.7 Minimization, Redaction, and Bounded Disclosure Discipline

Evidence access at every tier follows the minimization and redaction protocols established in Baseline C, applied to healthcare evidence categories.

Minimization Hierarchy:

1. **Tier 0:** All evidence aggregated and anonymized. No individual product, prescription, patient, or practitioner identifiable.

2. **Tier 1:** Evidence scoped to specific subjects. Products identified by CPO reference. Practitioners and patients pseudonymized. Commercial terms and pricing redacted. Clinical detail abstracted to evidence class presence/absence and status.
3. **Tier 2:** Full evidence access within approved scope. Practitioner and patient identity may be revealed where the objective trigger requires it. Commercial terms and clinical detail accessible where the investigation scope includes them.

Redaction for Evidence Pack Export. When evidence packs are exported for examination or dispute proceedings, automated redaction scans for prohibited data elements (per Baseline C's redaction protocol) and replaces them with redaction tokens. A redaction log documents what was redacted, when, by whom, and under what justification. The redaction log is included in the evidence pack as a separate artifact.

10.8 Optional Proof-Based Verification Where It Materially Improves Bounded Access

Where Baseline D's programmable privacy patterns are applied, proof-carrying compliance artifacts may replace certain reviewer queries, reducing the need for even Tier 1 evidence access.

Proof-Based Verification Applications:

Reviewer Query	Traditional Approach (Tier 1)	Proof-Based Alternative
"Is this product's authenticity verified?"	Retrieve PAES; examine provenance manifest; verify manufacturer credential	Verifier Output Pack (VOP) confirming VERIFIED authenticity state; reviewer validates VOP without accessing raw provenance evidence
"Is the prescriber's authority current?"	Retrieve AES; examine credential reference and revocation check	VOP confirming issuer legitimacy CONFIRMED within freshness window; no credential detail exposed
"Has the contraindication screening been performed?"	Retrieve SES; examine DS-01 evidence class	VOP confirming DS-01 evidence class present and current; no patient or clinical detail exposed
"Does this product have an active recall?"	Retrieve product recall/hold state records	VOP confirming ACTIVE state (no recall); no product-specific commercial or custody detail exposed

Operating Constraints for Proof-Based Verification:

- Proof-based verification supplements but does not replace the tiered access model. If the VOP is insufficient to answer the reviewer's question, standard Tier 1 or Tier 2 access remains available.
- Every VOP is stored as an ILS record with content-addressed integrity, freshness timestamps, and revocation status references per Baseline D conventions.
- Stale or revoked VOPs trigger re-verification; reviewers may not rely on expired proof outputs.

---

11. Governance, Change Control, Recertification, and Accountability

11.1 Governance Structure and Role Taxonomy

The governance structure for this framework follows the patterns established in Baselines B and C: distributed governance with defined roles, no single-party override capability, clear accountability assignments, and examiner-accessible governance records.

Governance Body Taxonomy (Adapted from Baseline B):

Governance Body	Role	Composition	Decision Authority
Framework Steering Committee	Strategic direction; standard approval; performance evaluation; escalated issue resolution	Institutional representatives, operational participants, independent experts, regulatory observers (non-voting)	Approve material changes to framework standards; evaluate performance; resolve escalated disputes
Change Control Board	Manage evolution of operational standards, evidence requirements, reconciliation cadences, and governance procedures	Technical experts from participating institutions and operational roles	Approve or reject change requests; coordinate implementation; manage version control
Incident Coordination Function	Facilitate coordinated response to incidents affecting multiple participants or revealing systemic issues	Rotating participation from operational entities; designated coordinator	Coordinate investigation; aggregate information; facilitate communication; document lessons learned
Conformance Assessment Function	Oversee conformance testing, evidence quality review, and participant readiness validation	Assessment personnel with relevant expertise; independent of assessed entities	Certification recommendations; deficiency identification; remediation oversight

No New Supervisory Bodies. This framework does not create new regulatory authorities, supervisory bodies, or institutional oversight structures beyond those implied by the baseline governance patterns. The governance bodies listed above are operational coordination structures — not regulatory entities. Regulatory authority, supervisory jurisdiction, and institutional oversight remain with existing bodies.

11.2 RACI Slices for Critical Activities

RACI matrices define accountability for critical operational activities. The RACI conventions follow Baseline C's RACI matrix structure. Healthcare-specific RACI slices cover activities not addressed in securities-focused baselines.

RACI Matrix — Product Authenticity and Provenance:

Activity	Manufacturer	Distributor	Pharmacy/ Hospital	Governance Body	Examiner Support
Generate CPO	R/A	I	I	I	I
Maintain provenance manifest	R	R	R (at their custody segment)	I	C
Verify product authenticity at receipt	I	R	R	I	I
Detect provenance break	C	R	R	I	C
Contain provenance break (hold-only)	C	R/A	R/A	C	I
Resolve provenance break	R	R	R	A	C

RACI Matrix — Authorization and Dispensation:

Activity	Prescriber	Dispensing Entity	Institutional Governance	Credentialing Body	Examiner Support
Issue authorization	R/A	I	I	I	I
Verify issuer legitimacy at dispensation	I	R/A	C	C	I
Execute dispensation precondition gates	I	R/A	I	I	I
Detect authorization break	I	R	C	C	C
Contain authorization break (hold-only)	I	R/A	C	I	I
Revoke authorization	R/A	I	A (if governance-initiated)	C	I

RACI Matrix — Recall and Correction:

Activity	Recall Authority	Custody Holders	Governance Body	Examiner Support
Initiate recall	R/A	I (notified)	I	I
Acknowledge recall	I	R	I	I
Quarantine affected products	I	R/A	I	I
Track recall scope completion	R	R (report inventory)	C	C
Close recall	R/A	I	A (approval)	I
Approve correction EP Delta	C	R	A	I

R = Responsible, A = Accountable, C = Consulted, I = Informed.

11.3 Authority and Delegation Controls

Authority to perform operational actions within the framework — modifying evidence, approving corrections, authorizing Tier 2 access, releasing holds, closing recalls — is governed by authority and delegation controls.

Authority Operating Rules:

- No single-party override. No individual entity or role can unilaterally modify evidence, override holds, or bypass governance controls. All material actions require multi-party authorization per the RACI matrices.
- Delegation must be documented. When authority is delegated (e.g., a senior pharmacist delegates dispensation approval to a staff pharmacist, or a governance body delegates change control authority to a working group), the delegation is recorded as an evidence artifact with: delegator identity, delegate identity, scope of delegation, temporal validity, and conditions for revocation.
- Delegation chains are limited. Multi-level delegation (A delegates to B, B delegates to C) is permitted only with explicit governance approval and documented justification. Each delegation level is independently auditable.
- Emergency delegation follows expedited approval. In emergencies, delegation may be activated on an expedited basis with post-hoc documentation, but the delegation must still be documented and the emergency conditions verified.

11.4 Material Change Triggers

Material changes — events or conditions requiring notification, re-evaluation, and documentation — are defined per Baseline D conventions, extended for healthcare contexts.

Material Change Trigger Catalog:

Trigger Category	Specific Triggers	Required Response
Product-level	New product safety information; batch/lot recall; manufacturer production change; formulation modification; packaging change	Re-assessment of affected PAES, SES; notification to downstream custody holders; governance documentation
Authorization-level	Prescriber credential revocation or restriction; institutional formulary change; regulatory reclassification of product	Re-assessment of affected AES; hold on pending dispensation where applicable; governance documentation
Custody-level	Custody entity loss of authorization; storage facility compromise; logistics provider change; new custody node onboarded	Re-assessment of affected CES; re-verification of custody chain integrity; governance documentation
Safety-level	Clinical decision-support algorithm update; interaction database major version change; new contraindication identified	Re-assessment of affected SES; notification to dispensation points; governance documentation

Trigger Category	Specific Triggers	Required Response
Governance-level	Change in governance body composition; change in authority delegation; change in reconciliation cadence; change in access policy	Governance documentation; stakeholder notification; recertification evaluation
Technology-level	Evidence storage system migration; content-addressing algorithm change; cryptographic algorithm update	Change control procedure per Section 11.4 and Baseline B's crypto-agility baseline; conformance re-testing

Material Change Response. Each material change trigger activates a standardized response: the trigger event is logged as a MATERIAL_CHANGE event in the ILS, the affected scope is identified, downstream impact is assessed, and the governance body determines whether recertification (Section 11.5) is required.

11.5 Recertification Cadence

Recertification is the periodic validation that operational controls, participant capabilities, evidence quality, and governance procedures continue to meet framework requirements. Recertification cadences follow Baseline D conventions.

Recertification Schedule:

Recertification Type	Default Cadence	Trigger for Off-Cycle Recertification	Evidence Produced
Participant operational readiness	Annual	Material change trigger affecting participant capabilities; SEV-1 or SEV-2 incident	Recertification report with conformance assessment; deficiency identification; remediation plan
Evidence quality assessment	Semi-annual	Repeated evidence integrity failures (3+ BRK-INTEG in 90 days); examiner finding of evidence gaps	Evidence quality audit report; gap inventory; remediation verification
Governance control effectiveness	Annual	Material change in governance body composition or authority delegation; governance violation detected	Governance control review report; RACI validation; delegation audit
Reconciliation framework effectiveness	Quarterly	Reconciliation break rates exceeding defined thresholds; new reconciliation type added	Reconciliation performance report; break trend analysis; cadence adjustment recommendations
Tiered access compliance	Annual	Post-access review finding of scope violation; overdue PARP; Tier 2 access frequency exceeding threshold	Access compliance report; PARP completion rates; scope violation inventory

---

11.6 Liability Trigger Catalog

A liability trigger is an operational condition that requires immediate action, escalation, and evidence preservation. The liability trigger catalog extends Baseline C's catalog with healthcare-specific triggers.

Healthcare Liability Trigger Catalog:

Trigger ID	Condition	Severity	Immediate Action	Evidence Requirement
LT-01	Confirmed counterfeit product detected in custody chain	Critical	Quarantine all affected units; incident escalation; regulatory notification	Preservation Bundle with all provenance and custody evidence
LT-02	Dispensation of product under active recall	Critical	Patient notification per institutional policy; corrective action; regulatory notification	Dispensation record, recall notification, acknowledgment evidence
LT-03	Authorization issued by entity with revoked credentials	High	Hold all pending dispensation under affected authorizations; investigation	AES with revocation evidence; affected dispensation inventory
LT-04	Evidence integrity failure suggesting deliberate tampering	Critical	Containment of affected evidence; incident investigation; governance notification	Integrity failure evidence; investigation records; affected state inventory
LT-05	Tier 2 access scope violation detected	High	Access terminated; post-access review escalated; governance notification	Access event records; scope deviation documentation
LT-06	Unresolved SEV-1 reconciliation break exceeding resolution SLA	High	Escalation to governance body; expanded investigation scope	Break detection records; investigation timeline; SLA documentation
LT-07	Silent overwrite of evidence artifact detected (no EP Delta)	Critical	Containment of affected evidence chain; integrity investigation	Original and modified artifact hashes; access logs; investigation records
LT-08	Dispensation precondition gate bypassed without documented override	High	Post-dispensation review; hold on future dispensation at affected point	Gate bypass evidence; dispensation record; override documentation (if any)

11.7 Incident Escalation and Containment

Incident escalation follows the tiered approach established in Baseline B's Incident Response Playbook, applied to healthcare operational incidents.

Escalation Tiers:

Incident Severity	Notification Timeline	Escalation Path	Containment Actions
Critical (LT-01, LT-02, LT-04, LT-07)	Governance body notified within 2 hours; regulatory notification per institutional policy	Incident Coordination Function → Governance Body → Regulatory liaison	Immediate hold-only containment; affected scope quarantine; Preservation Bundle initiated
High (LT-03, LT-05, LT-06, LT-08)	Governance body notified within 8 hours	Operational management → Incident Coordination Function → Governance Body if unresolved within SLA	Hold-only containment on affected downstream actions; Tier 1 investigation initiated
Moderate	Governance body notified within 24 hours	Operational management → Change Control Board if systemic issue	Investigation initiated; no hold unless escalation conditions met
Low	Included in periodic governance reporting	Operational management	Correction during next reconciliation cycle

Containment Principles. Containment actions are proportional, documented, and reversible. Hold-only containment restricts state changes but does not destroy evidence, modify records, or bypass governance controls. Containment scope is determined by the incident scope — not expanded beyond what the evidence supports.

11.8 No-Master-Key Posture and Distributed Approvals

The framework maintains a strict no-master-key posture inherited from Baselines A and B. No single entity, role, or key holder can unilaterally perform any of the following actions:

- Override hold-only containment without documented resolution and approval chain.
- Modify content-addressed evidence artifacts after storage.
- Bypass dispensation precondition gates.
- Grant Tier 2 reviewer access.
- Close a recall without governance approval.
- Execute a correction without documented authorization and EP Delta generation.
- Activate or deactivate legal hold without documented authority.

Distributed Approval Requirements. All material governance actions require approval from two or more independent parties per the RACI matrices. "Independent" means that the approving parties do not share reporting relationships, institutional affiliations, or financial interests that would compromise the independence of their judgment. Independence requirements are documented at governance body formation and verified at each recertification cycle.

11.9 Accountability for Corrections, Overrides, Recalls, and Supersession Events

Every correction, override, recall, and supersession event generates an accountability record documenting who took the action, under what authority, with what justification, and with what downstream impact.

Accountability Record — Minimum Fields:

Field	Description
event_id	Unique content-addressed identifier for the accountability record
event_type	CORRECTION, OVERRIDE, RECALL, SUPERSESSION, HOLD_RELEASE, GOVERNANCE_ACTION
actor_id	Pseudonymized or role-based identifier of the acting entity
authority_reference	Pointer to the governance approval, delegation instrument, or institutional authority under which the action was taken
justification	Documented reason for the action, with evidence references
affected_scope	Products, authorizations, custody chains, dispensation events, or evidence artifacts affected
downstream_impact_assessment	Assessment of downstream actions that relied on the prior state and may require adjustment
approval_chain	All approvals obtained, with approver identifiers and timestamps
timestamp	UTC timestamp of action execution
content_address	Self-referential hash of this accountability record

Accountability Record Retention. Accountability records are retained for the longest of: the retention period applicable to the affected evidence, the institutional governance retention requirement, and any applicable legal hold duration. Accountability records are never subject to shorter retention than the evidence they govern.

Accountability Record Access. Accountability records are accessible at Tier 0 (aggregate statistics: correction rates, override frequencies, recall counts) and at Tier 1 (specific accountability records for identified events under documented purpose code and TTL). Tier 2 access to underlying actor identities follows standard Tier 2 requirements.

---

12. Financially Consequential Workflows (Optional / Conditional Scope)

This section is included because the optional Baseline E (Payments & Settlement Constitution) materially improves coherence for healthcare claim, reimbursement, and payout workflows. Where financially consequential workflows are not in scope, this section may be omitted without affecting the remainder of the framework.

12.1 Claim and Reimbursement Event Taxonomy

Financially consequential events in healthcare workflows follow a defined lifecycle. Each event generates evidence artifacts stored as ILS records with content-addressed integrity, linked to underlying product, authorization, dispensation, and safety evidence.

Claim Lifecycle Event Taxonomy:

Event Code	Event Name	Description	Evidence Generated
CLM_SUBMITTED	Claim Submission	Claim for reimbursement submitted to benefit	Claim record with dispensation reference,

Event Code	Event Name	Description	Evidence Generated
		administrator or payer, referencing a specific dispensation event	authorization reference, product reference, claimant identification, amount
CLM_VALIDATED	Claim Validation	Claim validated against required evidence linkages — dispensation evidence exists, authorization is VALID, product authenticity is VERIFIED	Validation record with linkage check results per evidence category
CLM_ADJUDICATED	Claim Adjudication	Claim reviewed and determination issued (approved, denied, pended for additional information)	Adjudication record with determination, reason code, reviewed evidence references
CLM_APPROVED	Claim Approved	Claim approved for reimbursement or payout	Approval record with evidence sufficiency confirmation; all prerequisite states verified
CLM_DENIED	Claim Denied	Claim denied with documented reason and evidence references	Denial record with reason code, evidence references, appeal pathway documentation
CLM_PENDED	Claim Pended	Claim held pending resolution of evidence condition (missing evidence, stale evidence, disputed evidence)	Pend record with hold reason, required resolution actions, expected timeline
CLM_PAID	Claim Paid	Payout executed and settlement confirmed	Settlement confirmation with payment reference, amount, payout timing, linked approval record
CLM_ADJUSTED	Claim Adjusted	Previously paid claim subject to post-payment correction (overpayment, underpayment, retroactive evidence change)	Adjustment record with reason, amount delta, rebinding to corrected evidence chain
CLM_REVERSED	Claim Reversed	Previously paid claim fully reversed due to evidence invalidation (revoked authorization, recalled product, fraudulent claim)	Reversal record with reason, linked invalidation evidence, recovery initiation
CLM_APPEALED	Claim Appeal	Denied or adjusted claim appealed by claimant	Appeal submission with additional evidence or argumentation; appeal review initiated

Event Chaining. Claim lifecycle events form a content-addressed chain per Baseline C conventions. Each event record contains the content hash of the preceding event, the claim reference ID, and cross-references to the underlying dispensation, authorization, and product evidence. The complete claim chain is traversable for reviewer replay.

12.2 Evidence-Linked Release, Claim, or Reimbursement Gating

The central principle from Baseline E applies directly: financially consequential actions should not proceed when evidence states are materially unresolved. Claim progression from CLM_SUBMITTED to CLM_APPROVED requires that linked evidence states meet minimum completeness thresholds.

Claim Evidence Gate (Conceptual):

Gate	Verification Required	Failure Response
CG-1: Dispensation Evidence	Dispensation event record exists, is content-addressed, and references a valid dispensation precondition gate completion	Claim pended (CLM_PENDED); dispensation evidence gap documented
CG-2: Authorization Linkage	Referenced authorization state = VALID or EXPIRED-but-was-valid-at-dispensation-time; issuer legitimacy CONFIRMED at dispensation	Claim pended if authorization state unresolved; denied if authorization REVOKED pre-dispensation
CG-3: Product Authenticity	Referenced product authenticity state = VERIFIED at dispensation time	Claim pended if authenticity UNRESOLVED; denied if authenticity FAILED
CG-4: Safety Evidence	Proof-of-safety state = SUFFICIENT at dispensation time (required evidence classes present and current)	Claim pended if safety evidence INSUFFICIENT; review escalation if safety DISPUTED
CG-5: No Active Recall/Hold	Product not subject to active recall or hold at claim submission time	Claim pended if active recall; claim review initiated if recall occurred post-dispensation
CG-6: No Duplicate Claim	No prior paid claim exists for the same dispensation event	Claim denied as duplicate; existing paid claim referenced

Gate Execution. All gates are evaluated at CLM_VALIDATED. Gate results are logged as part of the validation record. A failure at any gate results in CLM_PENDED (for resolvable conditions) or CLM_DENIED (for conditions indicating the claim should not be paid). Gate results reference the specific evidence artifacts examined, enabling reviewer replay of the validation decision.

Temporal Evidence Assessment. Claim evidence gates assess evidence state at the time of the dispensation event, not at the time of claim submission. An authorization that was VALID at dispensation but has since EXPIRED does not block the claim — the gate confirms that the authorization was valid when the dispensation occurred. Conversely, an authorization that was REVOKED before the dispensation event blocks the claim even if it is currently shown as REVOKED (the revocation preceded the dispensation).

12.3 Settlement / Payout Linkage for Approved Claims

Approved claims progress to payout through evidence-linked settlement confirmation adapted from Baseline E's DvP finality model.

Payout Evidence Chain:

```
CLM_APPROVED
  → Payout instruction generated with:
    - claim_id (content address)
    - approval_record_reference (content address)
    - payout_amount
    - payee_reference
    - payment_method_reference
  → Payout execution confirmed with:
    - payment_reference (transaction ID from payment system)
    - execution_timestamp
    - amount_confirmed
    - settlement_status: SETTLED | FAILED | PENDING
  → CLM_PAID event generated linking:
    - claim approval to payout execution
    - complete evidence chain traversable from
      claim → dispensation → authorization → product → custody
```

Payout Finality. Consistent with Baseline E's treatment of settlement finality as an "evidence-backed condition, not an assertion," payout finality is documented through evidence artifacts — not claimed through system status alone. A CLM_PAID event is generated only when the payout execution confirmation is received and validated. Pending payouts remain in CLM_APPROVED state until execution is confirmed.

12.4 Hold or Segmentation Logic for Financially Unresolved States

When evidence conditions block claim progression, the framework applies hold or segmentation logic to prevent financially consequential actions on unresolved states.

Financial Hold Categories:

Hold Category	Trigger	Effect	Resolution Pathway
Evidence gap hold	Required evidence artifact absent or incomplete (CG-1 through CG-4 failure)	Claim held at CLM_PENDED; no payout	Evidence gap resolved; gate re-evaluated; claim progresses if gates pass
Recall hold	Product subject to active	Claim held; payout	Recall resolved (product

Hold Category	Trigger	Effect	Resolution Pathway
	recall at claim submission or between dispensation and claim	blocked	cleared or replacement dispensed); claim re-evaluated
Authorization dispute hold	Authorization validity disputed between parties	Claim held pending dispute resolution	Dispute resolved per Section 8.6; authorization state confirmed; claim re-evaluated
Duplicate detection hold	Potential duplicate claim identified (same dispensation, different claim IDs)	Both claims held pending investigation	Investigation confirms duplicate (one denied) or confirms distinct claims (both progress)
Post-payment correction hold	Evidence state changes after payout (authorization revoked, product recalled, dispensation evidence corrected)	Recovery assessment initiated; future claims from same source may be held	Adjustment (CLM_ADJUSTED) or reversal (CLM_REVERSED) executed per determination

Segmentation. Held claim amounts are logically segmented from payable amounts in benefit administration systems. Segmentation evidence is logged as ILS records documenting the segregation of held versus payable funds. This adapts Baseline E's escrow segmentation logic to healthcare reimbursement contexts.

12.5 Unmatched Claim / Unmatched Settlement / Unmatched Payout Breaks

Reconciliation between claim records, settlement records, and payout records may reveal unmatched items — claims without corresponding payouts, payouts without corresponding claims, or settlement amounts that do not match claim amounts.

Unmatched Item Taxonomy:

Unmatched Type	Description	Break Severity	Resolution
Claim without payout	CLM_APPROVED exists but no corresponding CLM_PAID within expected payout cycle	SEV-3 (Moderate) initially; escalates to SEV-2 if payout cycle exceeded by 2x	Investigation of payout system; re-submission if processing failure; escalation if systemic
Payout without claim	Payment record exists without corresponding approved claim	SEV-2 (High) — potential unauthorized payment	Immediate investigation; recovery if unauthorized; correction if claim record lost
Amount mismatch	CLM_PAID amount differs from CLM_APPROVED amount beyond tolerance	SEV-3 if within rounding tolerance; SEV-2 if material	Adjustment (CLM_ADJUSTED) for amount correction; investigation for systemic pricing errors
Duplicate payout	Multiple CLM_PAID events for single CLM_APPROVED	SEV-1 (Critical) — potential fraud or system error	Immediate investigation; recovery of duplicate amount; system control review

Unmatched Type	Description	Break Severity	Resolution
Orphaned adjustment	CLM_ADJUSTED exists without corresponding original CLM_PAID	SEV-2	Investigation of adjustment origin; correction or reversal per determination

Open Breaks Register. Adapted from Baseline E (Section 10.2): all unmatched items are maintained in an open breaks register for claim/reimbursement reconciliation. Breaks exceeding defined age thresholds trigger escalation, governance notification, and preservation bundle creation. The register is a mandatory component of the claim/reimbursement evidence pack.

12.6 Adjustment, Reversal, and Post-Correction Rebinding

When evidence changes after payout — an authorization is retroactively revoked, a product is recalled, or dispensation evidence is corrected — the framework provides structured adjustment and reversal pathways.

Adjustment Workflow:

1. **Trigger detection.** Upstream evidence change (authorization revocation, product recall, dispensation correction) detected through reconciliation or downstream propagation (Section 8.7).
2. **Impact assessment.** Affected claims identified through evidence linkage chain traversal. Financial impact quantified.
3. **Determination.** Adjustment authority determines appropriate response: partial adjustment (CLM_ADJUSTED with amount delta), full reversal (CLM_REVERSED), or no action (if upstream change does not materially affect claim validity).
4. **Execution.** Adjustment or reversal executed with evidence record linking to the upstream change that triggered it, the original claim and payout records, and the determination authority and justification.
5. **Rebinding.** If the upstream evidence is corrected (not invalidated), the claim evidence linkage is rebound to the corrected evidence through EP Delta. The original linkage is preserved as historical state per Section 3.9 conventions.
6. **Recovery.** If reversal creates a recovery obligation (funds to be returned), recovery initiation is logged and tracked in the open breaks register until recovered or written off per institutional policy.

Non-Destructive Correction. Consistent with Section 8.3: adjustments and reversals do not delete original claim or payout records. They create new events (CLM_ADJUSTED, CLM_REVERSED) linked to the originals through content-addressed references.

12.7 Operational Finality of Claim or Payout Evidence (Not Legal Finality)

Claim and payout finality within this framework is operational — it indicates that the evidence chain is complete, reconciled, and not subject to unresolved breaks. Operational finality does not constitute legal finality, adjudication of coverage rights, or waiver of adjustment or recovery rights.

Operational Finality Conditions for Claim Evidence:

Condition	Verification
Dispensation evidence complete and reconciled	PAES, AES, CES, SES cross-referenced and aligned
Authorization valid at dispensation time	Temporal evidence assessment confirms VALID state
Claim evidence gates passed	All CG gates passed at CLM_VALIDATED
Payout executed and confirmed	CLM_PAID event generated with settlement confirmation
No open breaks in claim evidence chain	Open breaks register shows zero unresolved items for this claim
Reconciliation current	Most recent claim-evidence reconciliation shows ALIGNED

Post-Finality Correction. Even after operational finality, corrections remain possible through the adjustment and reversal pathways (Section 12.6). Post-finality corrections follow enhanced governance procedures: multi-party approval, documented legal or contractual basis, and preservation of the complete pre-correction evidence chain. This adapts Baseline E's post-settlement correction protocol directly.

---

13. Offboarding, Legacy Compatibility, and Reversibility Without Data Loss

13.1 Offboarding Triggers

Offboarding is the controlled transition of product, authorization, custody, or safety evidence from the framework's evidence system to a legacy system — or the orderly wind-down of a participant's use of the framework. Offboarding may be triggered by:

Trigger	Description	Governance Requirement
Institutional decision	Participant decides to transition to alternative evidence management system	Governance notification; orderly transition per offboarding plan
Pilot conclusion	Framework pilot period ends; participants transition per program plan	Steering committee approval of offboarding plan; coordinated timeline
Participant non-conformance	Participant fails recertification or conformance requirements; cannot remediate within SLA	Governance determination; suspension followed by offboarding
Regulatory directive	Regulatory authority directs cessation of framework participation	Immediate compliance; offboarding per regulatory timeline
System decommission	Evidence storage or operational system decommissioned	Change control process; migration plan; offboarding of affected evidence scope
Product lifecycle end	Product withdrawn from market; no further dispensation, claim, or review expected	Transition to archival-only evidence management

Pre-Offboarding Requirements. Before offboarding execution begins: all active holds must be resolved or transferred; all open reconciliation breaks must be resolved or documented in the open breaks disclosure (Section 13.6); all pending claims must be adjudicated or transferred; and governance approval for offboarding must be documented.

13.2 Final State Snapshots

At offboarding initiation, the framework generates a comprehensive final state snapshot capturing the current state of all evidence within the offboarding scope.

Final State Snapshot Contents:

Component	Description	Format
Product evidence snapshot	Current PAES for all products within offboarding scope, including authenticity state, provenance state, and recall/hold status	Content-addressed manifest with artifact references
Authorization evidence snapshot	Current AES for all authorizations within scope, including validity state and supersession chain status	Content-addressed manifest with full supersession chains
Custody evidence snapshot	Current CES for all products within scope, including chain status and most recent custody event	Content-addressed manifest with custody chain endpoints
Safety evidence snapshot	Current SES for all products/decisions within scope, including evidence class currency status	Content-addressed manifest with evidence class references
Reconciliation posture snapshot	Most recent reconciliation results for all reconciliation types within scope	Content-addressed reconciliation reports
Open breaks snapshot	All unresolved breaks at offboarding initiation with status, severity, and investigation state	Open breaks register export
Claim/reimbursement snapshot (if Section 12 in scope)	All pending claims, open breaks register for claims, and recent claim lifecycle events	Content-addressed claim evidence manifest

Snapshot Integrity. The final state snapshot is content-addressed as a whole — a master hash covers all component manifests, enabling a single integrity verification of the complete snapshot. The snapshot is signed by the responsible officer per institutional governance.

13.3 Final Reconciliation Proof

After the final state snapshot is generated, a final reconciliation cycle is executed covering all evidence types within the offboarding scope.

Final Reconciliation Requirements:

- All reconciliation types from Section 9.5 are executed at the offboarding scope.

- All breaks detected in the final reconciliation are documented in the final reconciliation report.
- Breaks that can be resolved within the offboarding timeline are resolved through standard break resolution workflows (Section 9.6).
- Breaks that cannot be resolved before offboarding completion are documented as open breaks in the offboarding disclosure (Section 13.6).
- The final reconciliation report is content-addressed and signed by the responsible officer.

Final Reconciliation Report — Minimum Contents:

Element	Description
Reconciliation scope	Products, authorizations, custody chains, and evidence artifacts covered
Reconciliation types executed	All types from Section 9.5 cadence matrix
Alignment results per type	ALIGNED count, BREAK_DETECTED count per reconciliation type
Break inventory	All detected breaks with type, severity, and resolution status
Resolved breaks	Breaks resolved during final reconciliation with resolution evidence references
Unresolved breaks	Breaks carried forward as open breaks with justification for non-resolution
Reconciliation attestation	Responsible officer sign-off confirming completeness and accuracy
Report content address	Self-referential hash for integrity verification

---

13.4 Legacy Transition Manifest

The legacy transition manifest documents the mapping between the framework's evidence artifacts and the legacy system's record structure, enabling the receiving system to ingest, verify, and maintain the evidence chain.

Legacy Transition Manifest — Structure:

```
legacy_transition_manifest:
  manifest_id: [content_address]
  offboarding_scope: [description of scope]
  source_system: [framework identifier]
  target_system: [legacy system identifier]
  transition_timestamp: [UTC]
  mapping_table:
    - framework_artifact_type: PAES
      legacy_equivalent: [legacy product record type]
      field_mapping: [field-by-field mapping document reference]
      data_loss_assessment: [fields not representable in legacy; mitigation]
    - framework_artifact_type: AES
```

```
    legacy_equivalent: [legacy authorization record type]
    field_mapping: [field-by-field mapping document reference]
    data_loss_assessment: [fields not representable in legacy; mitigation]
  - ... [continued for all evidence types]
completeness_verification:
  total_artifacts_in_scope: [count]
  artifacts_successfully_mapped: [count]
  artifacts_with_data_loss: [count with descriptions]
  artifacts_not_mappable: [count with justification and archival plan]
transition_attestation:
  attesting_officer: [identity]
  attestation_timestamp: [UTC]
  attestation_statement: "The legacy transition mapping is complete and
    accurate. Data loss items are documented. Non-mappable artifacts are
    archived per retention policy."
manifest_content_address: [self-referential hash]
```

Data Loss Assessment. Where the legacy system cannot represent certain evidence fields (e.g., content-addressed integrity markers, hash chain linkage, tiered access metadata), the data loss assessment documents: what fields are lost, what operational capability is affected, and what mitigation is applied (typically: archival of the complete framework evidence alongside the legacy records, enabling retrieval of the full evidence chain from the archive if needed post-offboarding).

13.5 Portable Evidence Set and Bounded Transfer

Evidence transfer to the legacy system or successor system follows bounded transfer principles — only evidence within the offboarding scope is transferred; evidence outside scope remains in the framework.

Bounded Transfer Rules:

- Evidence is transferred as content-addressed artifacts with integrity verification at both source and destination.
- The transfer is logged as a chain-of-custody event for the evidence artifacts: source system, destination system, transfer timestamp, transferring authority, and integrity verification results at both endpoints.
- The receiving system acknowledges ingestion and confirms record counts and integrity verification results. Ingestion acknowledgment is logged as part of the offboarding evidence.
- Evidence not accepted by the receiving system (format incompatibility, integrity failure, unmappable fields) is documented in the transition manifest and archived in the framework's storage per retention policy.

Post-Transfer Verification. After transfer, a verification step confirms that the legacy system's records accurately reflect the framework's evidence at the point of transition. Verification includes: record count comparison, key field value spot-checks, and integrity verification of content-addressed artifacts where the legacy system supports content addressing.

13.6 Open-Break Disclosure Requirements

If unresolved reconciliation breaks exist at offboarding completion, they must be disclosed in the offboarding documentation.

Open-Break Disclosure — Required Contents:

Element	Description
Break inventory	All unresolved breaks with break ID, type, severity, and description
Investigation status	Current investigation status for each break; evidence gathered to date
Reason for non-resolution	Documented reason why the break could not be resolved before offboarding (time constraint, evidence unavailability, dispute pending)
Impact assessment	Assessment of each break's potential impact on product integrity, authorization validity, claim accuracy, or safety evidence
Mitigation plan	Actions to address each break post-offboarding (continued investigation, monitoring, escalation to governance)
Accountable party	Entity responsible for each break's post-offboarding resolution
Disclosure attestation	Responsible officer sign-off confirming that all known breaks are disclosed and no breaks are concealed

Zero-Break Preference. Adapted from Baseline E (Section 10.2): the offboarding proof bundle requires open breaks = 0 or an explicit, approved break list. Where open breaks exist, governance approval for offboarding with open breaks must be documented, including acknowledgment of the associated risks.

13.7 Archival Retention and Post-Offboarding Monitoring

After offboarding completion, the framework's copy of the evidence is archived — not deleted — with retention policies consistent with institutional requirements.

Archival Retention Requirements:

Evidence Category	Minimum Retention Post-Offboarding	Access Conditions
Product authenticity and provenance evidence	7 years post-offboarding or per institutional policy (whichever is longer)	Tier 1 or Tier 2 access per standard tiered access requirements
Authorization evidence	7 years post-offboarding	Same
Custody evidence	7 years post-offboarding	Same
Safety evidence and clinical decision records	10 years post-offboarding or per institutional policy (alignment objective: match product liability window)	Same; enhanced preservation for adverse event records
Claim/reimbursement	7 years post-offboarding	Same

Evidence Category	Minimum Retention Post-Offboarding	Access Conditions
evidence (if Section 12 in scope)		
Offboarding proof bundle	Indefinite (or per institutional archival policy)	Tier 1 access under documented purpose code
Preservation bundles (incident-related)	Indefinite	Tier 1 or Tier 2 access

Post-Offboarding Monitoring. For a defined monitoring period after offboarding (alignment objective: 12 months), the framework maintains visibility into:

- Open break resolution status (breaks disclosed under Section 13.6 tracked to closure).
- Recall or safety notifications affecting products that were in scope during framework operation.
- Examiner or regulatory requests for evidence from the offboarded scope.
- Integrity verification of archived evidence (periodic hash verification per reconciliation cadence).

Post-offboarding monitoring is conducted at reduced cadence (alignment objective: monthly rather than continuous) but follows the same evidence and governance discipline as active operations.

---

14. Examiner Readiness: Standard Checks Pack + Reviewer / Examiner Query Pack

14.1 Authenticity Checks

Standard checks for product authenticity verification, aligned with the examiner query pack structure from Baselines A and C.

Check ID	Check Purpose	Evidence Required	Pass Criteria	Fail Criteria	Severity
AUTH-001	Verify CPO exists for all products in scope	CPO registry; PAES manifests	100% of dispensed products have CPO with content-addressed integrity	Any product dispensed without CPO	High
AUTH-002	Verify manufacturer identity evidence current	AES for manufacturer credential; freshness check records	Manufacturer credential verified within applicable freshness window	Manufacturer credential expired or unverified at dispensation	High
AUTH-003	Verify provenance manifest completeness	Provenance manifests for sampled products	Sampled provenance manifests show COMPLETE chain status; no unresolved gaps	Any sampled manifest shows BROKEN or PARTIAL without documented investigation	Critical
AUTH-004	Verify content-addressed integrity	Hash chain verification	100% hash chain verifications pass for	Any hash chain failure	Critical

Check ID	Check Purpose	Evidence Required	Pass Criteria	Fail Criteria	Severity
	of provenance chain	results	sampled products		
AUTH-005	Verify authenticity state accurately reflects evidence	PAES with state determination; supporting evidence	Authenticity state consistent with evidence (VERIFIED only when all evidence elements present)	Authenticity state VERIFIED but evidence elements missing or stale	High

14.2 Provenance and Custody Checks

Check ID	Check Purpose	Evidence Required	Pass Criteria	Fail Criteria	Severity
PROV-001	Verify custody event chain completeness for sampled products	CES for sampled products	No undocumented custody gaps in sampled chains	Custody gap detected without corresponding break record	High
PROV-002	Verify handoff confirmation from both sender and receiver	CUS_HANDOFF and CUS_RECEIPT event pairs	All sampled handoffs have matching sender/receiver confirmations	Handoff without matching receipt or receipt without matching handoff	High
PROV-003	Verify storage condition monitoring active during storage periods	Storage condition logs; excursion records	Continuous condition records present for all storage periods; excursions documented and assessed	Storage periods without condition records; excursions without assessment	Moderate–High
PROV-004	Verify repackaging events authorized	CUS_REPACKAGE events; repackager credential evidence	All repackaging events linked to authorized repackager credential	Repackaging event without authorized entity credential	High
PROV-005	Verify aggregation hierarchy maintained	Aggregation linkage records; disaggregation event logs	All child units traceable to parent aggregation; no orphaned units	Units not traceable to parent; aggregation breaks	Moderate
PROV-006	Verify custody chain integrity at recall scope determination	Recall scope records; custody chain traversal results	All affected units identified through aggregation hierarchy; current custodians notified	Recall scope incomplete; units not accounted for	Critical

14.3 Authorization and Issuer-Legitimacy Checks

Check ID	Check Purpose	Evidence Required	Pass Criteria	Fail Criteria	Severity
ISSU-001	Verify issuer legitimacy confirmed at dispensation	AES linked to dispensation events	All sampled dispensation events linked to AES with legitimacy state CONFIRMED	Dispensation without issuer legitimacy verification	Critical
ISSU-002	Verify authorization freshness at dispensation time	AES freshness check timestamps; freshness window configuration	Issuer credential verified within applicable freshness window at dispensation time	Credential verification stale beyond freshness window at dispensation	High
ISSU-003	Verify revocation check performed at dispensation	Revocation check records in AES	Revocation check logged for each dispensation; result CLEAR or appropriately handled	Dispensation without revocation check; or REVOKED result without hold action	Critical
ISSU-004	Verify scope-match between authorization and dispensation	Scope-match verification records	Authorization bounds (product, quantity, location, purpose) match dispensation parameters	Scope mismatch without documented override or correction	High
ISSU-005	Verify supersession chain integrity for multi-version authorizations	Supersession chain records	Ordered chain; no ambiguous current-reference state; dispensation bound to current version	Dispensation bound to superseded authorization without re-verification	High
ISSU-006	Verify delegation authority where delegated prescribing applies	Delegation records; delegator AES	Delegation instrument current; delegator authority verified; delegation scope matches action	Delegation expired, delegator authority unverified, or scope exceeded	High

---

14.4 Proof-of-Safety and Review-State Checks

Check ID	Check Purpose	Evidence Required	Pass Criteria	Fail Criteria	Severity
SAFE-001	Verify required safety evidence classes present at dispensation	SES for sampled dispensation events	All required evidence classes (per Section 7.2 matrix) present for sampled events	Required evidence class absent for dispensation event	High
SAFE-002	Verify safety evidence currency at dispensation	Evidence class timestamps; source data	Evidence classes current relative to source data version	Evidence class generated against outdated source data;	High

Check ID	Check Purpose	Evidence Required	Pass Criteria	Fail Criteria	Severity
	time	version references	at dispensation time	not refreshed	
SAFE-003	Verify safety alert overrides documented	Safety alert records; override documentation	All overrides linked to DS-05 (prescriber clinical rationale) with documented justification	Override without documentation; or documentation inadequate per review posture	Critical
SAFE-004	Verify context-bound decision state records for high-impact decisions	Decision state records per Section 7.3	High-impact decisions have complete context-bound decision state records with all required fields	High-impact decision without decision state record or with incomplete fields	High
SAFE-005	Verify decision state replay capability	Decision state records; referenced evidence artifacts	Sampled decision states can be independently reconstructed from evidence references	Evidence referenced by decision state unavailable or integrity-failed	High
SAFE-006	Verify superseded safety evidence triggers appropriate action	Safety evidence supersession records; downstream dispensation events	Dispensation events after evidence supersession reference refreshed (not superseded) evidence	Dispensation relying on superseded safety evidence without refresh	High

---

14.5 Recall / Quarantine / Correction Checks

Check ID	Check Purpose	Evidence Required	Pass Criteria	Fail Criteria	Severity
RCLL-001	Verify recall scope determination complete	Recall initiation records; scope determination; aggregation hierarchy traversal	All affected units identified; all current custody holders notified	Scope determination incomplete; holders not notified	Critical
RCLL-002	Verify recall acknowledgment tracking	CUS_RECALL_ACK events; acknowledgment tracking records	All notified custody holders acknowledged within SLA	Acknowledgment missing or overdue without escalation	High
RCLL-003	Verify recalled products quarantined	CUS_QUARANTINE_ENTRY events for recalled products	All identified affected units quarantined or returned or destroyed	Recalled units not quarantined; disposition unknown	Critical
RCLL-004	Verify corrections generate EP Deltas	Correction records; EP Delta artifacts	All corrections produce EP Deltas with prior state preserved	Correction without EP Delta; or prior state not preserved (silent overwrite)	Critical
RCLL-005	Verify correction approval chain	Correction approval records	All material corrections approved	Correction without required approval	High

Check ID	Check Purpose	Evidence Required	Pass Criteria	Fail Criteria	Severity
	documented		by appropriate authority per RACI		
RCLL-006	Verify downstream propagation of corrections	Propagation records; affected downstream event inventory	All downstream events affected by correction identified and addressed	Downstream events referencing pre-correction state without update	High

---

14.6 Bounded-Access Compliance Checks

Check ID	Check Purpose	Evidence Required	Pass Criteria	Fail Criteria	Severity
ACCS-001	Verify all Tier 2 access events have dual-control approval	Tier 2 access event records; approval records	All Tier 2 access events have documented dual-control approval with independent approvers	Tier 2 access without dual-control approval	Critical
ACCS-002	Verify TTL enforcement for Tier 1 and Tier 2 access	Access event records; TTL expiration records	All access grants expired at TTL; no access beyond TTL without renewal	Access continuing beyond TTL without documented renewal	High
ACCS-003	Verify post-access review completion for Tier 2 events	Post-Access Review Pack (PARP) records	All Tier 2 access events have completed PARP within 5-business-day SLA	PARP missing, incomplete, or overdue	High
ACCS-004	Verify purpose limitation compliance	Access event purpose codes; evidence accessed	Evidence accessed consistent with documented purpose code; no scope creep	Evidence accessed outside documented purpose scope	High
ACCS-005	Verify minimization and redaction in evidence pack exports	Exported evidence packs; redaction logs	Prohibited data elements redacted; minimization techniques applied; redaction logged	Prohibited data elements present in exported evidence; missing redaction log	High
ACCS-006	Verify Tier 0 outputs contain no individual-identifiable data	Tier 0 report samples	Sampled Tier 0 outputs contain only aggregate statistics; no individual product, patient, or practitioner identifiable	Individual-identifiable data in Tier 0 output	High

---

14.7 Governance and Recertification Checks

Check ID	Check Purpose	Evidence Required	Pass Criteria	Fail Criteria	Severity
GOVN-001	Verify recertification completed per cadence	Recertification records; cadence schedule	All recertification cycles completed on schedule; no overdue recertifications	Overdue recertification without documented extension	High
GOVN-002	Verify material change triggers	Material change event records; governance	All material change triggers logged;	Material change without trigger	High

Check ID	Check Purpose	Evidence Required	Pass Criteria	Fail Criteria	Severity
	documented	response records	governance response documented within SLA	documentation or governance response	
GOVN-003	Verify no-master-key posture maintained	Governance action records; approval chains	All material governance actions have multi-party approval; no single-party override detected	Single-party override of governance control	Critical
GOVN-004	Verify RACI accountability for critical activities	RACI matrices; operational records for sampled activities	Sampled activities executed per RACI assignments; accountability documented	Activity executed by unauthorized party or without required accountable approval	High
GOVN-005	Verify liability trigger catalog maintained and current	Liability trigger catalog; trigger event records	Catalog current; all trigger events logged and responded to per catalog requirements	Trigger events not logged or response not per catalog	High

---

14.8 Offboarding Checks

Check ID	Check Purpose	Evidence Required	Pass Criteria	Fail Criteria	Severity
OFFB-001	Verify final state snapshot generated and integrity-verified	Final state snapshot manifest; integrity verification results	Snapshot complete; master hash verified; officer attestation present	Snapshot incomplete or integrity verification failed	High
OFFB-002	Verify final reconciliation executed and documented	Final reconciliation report	All reconciliation types executed; results documented; breaks inventoried	Final reconciliation incomplete or undocumented	High
OFFB-003	Verify open breaks disclosed	Open-break disclosure document; governance approval	All unresolved breaks disclosed; governance approved offboarding with open breaks	Undisclosed open breaks discovered post-offboarding	Critical
OFFB-004	Verify legacy transition manifest complete	Legacy transition manifest; field mapping; data loss assessment	All evidence types mapped; data loss documented; non-mappable artifacts archived	Evidence types not mapped; data loss not documented	High
OFFB-005	Verify post-transfer verification completed	Verification records; record count comparisons; integrity checks	Legacy system records match framework evidence at transition point	Verification failed or not performed	High
OFFB-006	Verify archival retention applied	Archival records; retention metadata	All evidence archived per retention requirements; no premature	Evidence destroyed before retention period; archive incomplete	High

Check ID	Check Purpose	Evidence Required	Pass Criteria	Fail Criteria	Severity
			destruction		

14.9 Conceptual Query Families (SQL / Pseudocode / Retrieval Logic)

This section provides conceptual query patterns that reviewers can adapt to their specific retrieval infrastructure. Queries reference the evidence taxonomy and event codes defined throughout this framework.

Query Family 1: Product Authenticity and Provenance

```
-- QRY-PAES-001: Retrieve authenticity state for a product at a specific time
SELECT p.product_reference_id, p.authenticity_state, p.state_timestamp,
       p.paes_manifest_hash, p.provenance_chain_status
FROM product_authenticity_states p
WHERE p.cpo_content_address = :target_cpo
  AND p.state_timestamp <= :target_timestamp
ORDER BY p.state_timestamp DESC
LIMIT 1;

-- QRY-PROV-001: Identify all custody gaps for a product
SELECT ce.event_id, ce.event_type, ce.timestamp, ce.actor_id,
       ce.previous_event_hash,
       CASE WHEN ce.previous_event_hash != lag_hash THEN 'GAP_DETECTED'
            ELSE 'CHAIN_INTACT' END AS chain_status
FROM custody_events ce
LEFT JOIN (
    SELECT event_id, content_address AS lag_hash
    FROM custody_events
) prev ON ce.previous_event_hash = prev.lag_hash
WHERE ce.product_cpo_reference = :target_cpo
ORDER BY ce.timestamp;

-- QRY-PROV-002: Count products with unresolved provenance breaks
SELECT COUNT(DISTINCT pm.cpo_reference) AS products_with_breaks
FROM provenance_manifests pm
WHERE pm.chain_status IN ('PARTIAL', 'BROKEN')
  AND pm.manifest_timestamp >= :period_start
```

```
  AND pm.manifest_timestamp <= :period_end;
```

Query Family 2: Authorization and Dispensation

```
-- QRY-AUTH-001: Verify authorization validity at dispensation time
SELECT d.dispensation_event_id, d.timestamp AS dispensation_time,
       a.authorization_id, a.validity_state AS auth_state_at_dispensation,
       a.issuer_legitimacy_state, a.freshness_status
FROM dispensation_events d
JOIN authorization_states a ON d.authorization_reference = a.authorization_id
  AND a.state_timestamp <= d.timestamp
  AND a.state_timestamp = (
      SELECT MAX(a2.state_timestamp) FROM authorization_states a2
      WHERE a2.authorization_id = d.authorization_reference
        AND a2.state_timestamp <= d.timestamp
  )
WHERE d.timestamp >= :period_start AND d.timestamp <= :period_end;

-- QRY-AUTH-002: Identify dispensation events with stale issuer verification
SELECT d.dispensation_event_id, d.timestamp,
       aes.currency_check_timestamp,
       EXTRACT(DAY FROM d.timestamp - aes.currency_check_timestamp)
         AS days_since_verification
FROM dispensation_events d
JOIN authorization_evidence_sets aes
  ON d.authorization_reference = aes.authorization_reference
WHERE EXTRACT(DAY FROM d.timestamp - aes.currency_check_timestamp)
  > :freshness_window_days
  AND d.timestamp >= :period_start;
```

Query Family 3: Safety Evidence and Decision Replay

```
-- QRY-SAFE-001: Verify required safety evidence classes present
SELECT d.dispensation_event_id, d.product_cpo_reference,
       ses.evidence_class, ses.status, ses.freshness_status
FROM dispensation_events d
CROSS JOIN required_evidence_classes rec
LEFT JOIN safety_evidence_sets ses
  ON d.dispensation_event_id = ses.dispensation_reference
```

```
  AND rec.evidence_class = ses.evidence_class
WHERE d.timestamp >= :period_start
  AND ses.evidence_class IS NULL;  -- returns missing evidence classes

-- QRY-SAFE-002: Retrieve context-bound decision states with overrides
SELECT ds.decision_id, ds.decision_type, ds.decision_timestamp,
       ds.override_flag, ds.override_justification,
       ds.algorithm_version, ds.output_result
FROM decision_states ds
WHERE ds.override_flag = TRUE
  AND ds.decision_timestamp >= :period_start
ORDER BY ds.decision_timestamp;
```

Query Family 4: Reconciliation and Break Management

```
-- QRY-RECON-001: Open breaks inventory with aging
SELECT b.break_id, b.break_type, b.severity, b.detected_at,
       EXTRACT(DAY FROM CURRENT_TIMESTAMP - b.detected_at) AS age_days,
       b.investigation_status, b.assigned_to
FROM reconciliation_breaks b
WHERE b.lifecycle_status NOT IN ('RESOLVED', 'CLOSED')
ORDER BY b.severity, b.detected_at;

-- QRY-RECON-002: Break resolution SLA compliance
SELECT b.severity,
       COUNT(*) AS total_breaks,
       SUM(CASE WHEN b.resolution_time <= b.sla_target THEN 1 ELSE 0 END)
         AS within_sla,
       ROUND(SUM(CASE WHEN b.resolution_time <= b.sla_target THEN 1 ELSE 0 END)
         * 100.0 / COUNT(*), 1) AS sla_compliance_pct
FROM reconciliation_breaks b
WHERE b.detected_at >= :period_start
  AND b.lifecycle_status IN ('RESOLVED', 'CLOSED')
GROUP BY b.severity;
```

Query Family 5: Tiered Access Compliance

```
-- QRY-ACCS-001: Tier 2 access events without completed PARP
SELECT ta.access_event_id, ta.timestamp, ta.actor_id,
```

```
       ta.purpose_code, ta.ttl_expiry,
       parp.review_timestamp AS parp_completed_at
FROM tier2_access_events ta
LEFT JOIN post_access_review_packs parp
  ON ta.access_event_id = parp.access_event_reference
WHERE parp.review_timestamp IS NULL
   OR parp.review_timestamp > ta.ttl_expiry + INTERVAL '5 days';

-- QRY-ACCS-002: Purpose code distribution for reviewer access
SELECT ta.purpose_code, ta.tier_level, COUNT(*) AS access_count,
       AVG(EXTRACT(HOUR FROM ta.ttl_expiry - ta.timestamp)) AS avg_ttl_hours
FROM all_access_events ta
WHERE ta.timestamp >= :period_start
GROUP BY ta.purpose_code, ta.tier_level
ORDER BY access_count DESC;
```

Query Family 6: Claim and Reimbursement (Optional — Section 12)

```
-- QRY-CLM-001: Claims with evidence gate failures
SELECT c.claim_id, c.submission_timestamp, c.claim_status,
       cg.gate_id, cg.gate_result, cg.failure_reason
FROM claims c
JOIN claim_evidence_gates cg ON c.claim_id = cg.claim_id
WHERE cg.gate_result = 'FAIL'
  AND c.submission_timestamp >= :period_start;

-- QRY-CLM-002: Post-payment adjustments and reversals
SELECT c.claim_id, c.original_amount, adj.adjustment_amount,
       adj.adjustment_reason, adj.upstream_change_reference,
       adj.adjustment_timestamp
FROM claim_adjustments adj
JOIN claims c ON adj.claim_id = c.claim_id
WHERE adj.adjustment_timestamp >= :period_start
ORDER BY adj.adjustment_timestamp;
```

---

15. Worked Examples (Paste-Ready)

15.1 Medicine Provenance Verification with Unresolved Substitution Risk and Hold-Only Containment

Scenario. Regional Distributor D receives a shipment of 5,000 units of Product X (an injectable biologic, narrow therapeutic index) from Manufacturer M. At receiving verification (CUS_RECEIPT), the automated product identity check flags a discrepancy: the batch/lot reference on the physical packaging does not match the batch/lot reference in the provenance manifest transmitted electronically by Manufacturer M.

Timeline:

Time (UTC)	Event	Actor	Evidence Generated
T+0:00	Shipment received at Distributor D warehouse	Distributor D receiving dock	CUS_RECEIPT initiated; physical inspection record
T+0:15	Automated CPO verification flags batch/lot mismatch: physical label shows LOT-2026-0488; provenance manifest references LOT-2026-0487	Distributor D verification system	BRK-PROV (provenance break) detection record; severity assessment: SEV-2 (High) — narrow therapeutic index product
T+0:20	Hold-only containment applied to all 5,000 units	Distributor D compliance	CUS_HOLD_ENTRY: hold_reason = "BATCH_LOT_MISMATCH"; affected_units = 5000; hold_authority = "COMPLIANCE_OFFICER_D"
T+0:25	Manufacturer M notified; investigation initiated	Distributor D → Manufacturer M	Investigation initiation record; notification evidence
T+4:00	Manufacturer M responds: labeling error confirmed — physical labels printed with LOT-0488, but production records confirm product is LOT-0487; provides corrected labeling documentation and production release certificate	Manufacturer M quality function	Manufacturer correction evidence: production release cert (content-addressed), corrected label attestation
T+6:00	Distributor D quality assessment confirms product integrity not affected (labeling error only; product itself is correct formulation and batch)	Distributor D quality function	Quality assessment record with determination: "labeling discrepancy — no product integrity impact"
T+8:00	Correction EP Delta generated: CPO updated	Distributor D + Manufacturer M	EP Delta: previous_state = BRK-PROV detected; new_state = RECONSTRUCTED;

Time (UTC)	Event	Actor	Evidence Generated
	with labeling note; provenance manifest annotation added		correction_authority = "MANUFACTURER_M_QUALITY + DISTRIBUTOR_D_QUALITY"
T+8:30	Hold released; product re-enters dispensable inventory with VERIFIED authenticity state	Distributor D compliance	CUS_HOLD_RELEASE: resolution_evidence = [correction EP Delta, quality assessment, manufacturer attestation]; approval_chain = [compliance_officer_D, quality_manager_D]
T+9:00	Post-resolution reconciliation confirms alignment; break lifecycle closed	Distributor D surveillance	Break closure record: BREAK-HC-2026-0112; resolution_time = 9h; root_cause = "labeling_print_error"

Evidence Artifacts Produced:

- CUS_RECEIPT with verification failure (ILS)
- BRK-PROV detection record with SEV-2 classification (ILS)
- CUS_HOLD_ENTRY with scope and authority (ILS)
- Manufacturer correction documentation (content-addressed)
- Quality assessment record (content-addressed)
- Correction EP Delta linking original break to resolution (content-addressed)
- CUS_HOLD_RELEASE with approval chain (ILS)
- Break closure record (ILS)
- Preservation Bundle (PB-BREAK-HC-2026-0112) containing all above artifacts

Examiner Replay Query: "Show complete timeline for break BREAK-HC-2026-0112 from detection through closure, including manufacturer response evidence and hold lifecycle."

15.2 Prescription Legitimacy Review with Expiry or Revocation Ambiguity Requiring Bounded Reviewer Escalation

Scenario. Pharmacy P receives a refill request for Patient Q's chronic medication (Product Y, 90-day supply). The dispensation precondition gate (G2: Authorization Validity) flags the prescription: the prescribing physician's credential was updated 15 days ago, and the update record is ambiguous — it could indicate a routine renewal or a scope restriction affecting Product Y's therapeutic category.

Timeline:

Time (UTC)	Event	Actor	Evidence Generated
T+0:00	Refill request submitted for Patient Q, Product Y	Pharmacy P dispensation system	Dispensation request record
T+0:02	Gate G2 check: AES for prescriber Dr. R retrieved; currency_check_timestamp = 15 days ago;	Pharmacy P gate engine	Gate G2 result: PENDED; reason = "ISSUER_CREDENTIAL_UPDATE_AMBIGUOUS"

Time (UTC)	Event	Actor	Evidence Generated
	credential update detected but update_type = AMBIGUOUS (system cannot determine renewal vs. restriction)		
T+0:03	Dispensation blocked; hold-only containment on this refill event	Pharmacy P compliance	Hold record: pending authorization review
T+0:10	Tier 1 reviewer access requested: purpose_code = PUR-RECON-BREAK; scope = Dr. R's AES and credential update record; TTL = 14 days	Pharmacy P compliance officer	Tier 1 access request record with justification
T+0:15	Tier 1 access granted; reviewer examines Dr. R's AES (pseudonymized at Tier 1: "PRESCRIBER_REF_4821")	Access approver	Access grant record; TTL assigned
T+2:00	Tier 1 review determines: credential update was a scope restriction — Dr. R's authority for Product Y's therapeutic category was narrowed effective 15 days ago; the active prescription was issued before the restriction	Reviewer	Review finding record: "Prescription issued under valid authority pre-restriction; prescription itself not revoked; however, refill authority may be affected"
T+3:00	Determination: prescription valid at issuance (pre-restriction); refill requires re-assessment because prescriber's current scope no longer covers Product Y category; escalation to prescriber or authorized substitute	Pharmacy P clinical pharmacist	Determination record: "Refill held pending prescriber re-authorization or transfer to authorized prescriber"
T+24:00	Dr. R confirms: refers Patient Q to Dr. S (authorized for Product Y category); Dr. S issues new prescription superseding Dr. R's original	Dr. R → Dr. S	Supersession record: Dr. R's prescription → SUPERSEDED; Dr. S's prescription → VALID; AES for Dr. S: legitimacy CONFIRMED, scope covers Product Y
T+25:00	Dispensation precondition	Pharmacy P	Gate completion record: all gates PASS

Time (UTC)	Event	Actor	Evidence Generated
	gates re-evaluated against Dr. S's prescription: all gates pass	gate engine	
T+25:15	Dispensation executed; refill released to Patient Q	Pharmacy P	CUS_DISPENSATION event; dispensation evidence record with all gate results
T+25:30	Post-access review for Tier 1 access completed; PARP generated	Independent reviewer	PARP: access scope verified; no scope deviation; finding supported the hold; prescriber notification occurred appropriately

Evidence Artifacts Produced:

- Dispensation request and gate failure records (ILS)
- Tier 1 access request, grant, and PARP (ILS)
- Review finding and determination records (content-addressed)
- Supersession chain: Dr. R prescription → SUPERSEDED → Dr. S prescription (CURRENT)
- Dr. S AES with legitimacy CONFIRMED (content-addressed)
- Gate completion and dispensation records (ILS)

15.3 Dispensation Workflow with Stale Custody Evidence Triggering Containment and Replay

Scenario. Hospital H's automated dispensation system initiates release of Product Z (a controlled substance) from the hospital pharmacy's automated dispensing cabinet to Clinical Unit 4. Gate G4 (Custody Integrity) detects that the most recent custody event for Product Z in this cabinet is 96 hours old — exceeding the 72-hour freshness threshold for controlled substance custody evidence.

Timeline:

Time (UTC)	Event	Actor	Evidence Generated
T+0:00	Dispensation request for Product Z to Clinical Unit 4	Hospital H ordering system	Dispensation request record
T+0:01	Gate G4 check: CES freshness review — last custody event (CUS_STORAGE_ENTRY) timestamp = T-96h; freshness threshold for controlled substances = 72h	Hospital H gate engine	Gate G4 result: FAIL; reason = "STALE_CUSTODY_EVIDENCE_96H_VS_72H_THRESHOLD"
T+0:02	Dispensation blocked; hold-only containment	Hospital H pharmacy system	Hold record: "Custody evidence stale; re-verification required before controlled substance release"
T+0:30	Hospital pharmacist performs manual custody verification: physical count of Product Z in cabinet matches system records;	Hospital H pharmacist	Manual custody verification record: physical_count = MATCH; access_log_review = NO_ANOMALY; verification_method = "MANUAL_COUNT_AND_ACCESS_LOG_REVIEW"

Time (UTC)	Event	Actor	Evidence Generated
	cabinet access logs reviewed — no unauthorized access detected		
T+0:45	Fresh custody event generated: CUS_STORAGE_EXIT from automated cabinet with manual verification attestation	Hospital H pharmacy system + pharmacist	CUS_STORAGE_EXIT with manual verification linkage; custody chain updated
T+0:50	Gate G4 re-evaluated: custody evidence now current (timestamp = T+0:45); all gates pass	Hospital H gate engine	Gate completion record: all gates PASS; G4 note = "Re-verified after stale evidence hold"
T+0:55	Dispensation executed under Enhanced review posture (controlled substance + hold event = elevated evidence preservation)	Hospital H pharmacy	CUS_DISPENSATION with Enhanced review posture classification

Key Evidence Pattern: The stale custody evidence did not indicate a safety problem — it indicated an evidence gap. The framework's response was proportional: hold-only containment until fresh evidence obtained, then release. The manual verification pathway (Section 7.6) provided the evidence refresh without requiring system replacement.

15.4 High-Impact Clinical-Decision Support Output Reviewed Under Minimal Disclosure Constraints

Scenario. Clinical Decision-Support System (CDSS) at Hospital H generates a contraindication alert for Patient P: the system detects a potential interaction between newly prescribed Product A and Patient P's existing medication Product B. The prescribing physician overrides the alert and authorizes dispensation. Six months later, a quality review examines override patterns for this CDSS version.

Decision State at Override (T+0):

```
context_bound_decision_state:
  decision_id: DS-HC-2026-07821
  decision_type: CONTRAINDICATION_OVERRIDE
  decision_timestamp: 2026-03-15T09:22:00Z
  decision_actor: PRESCRIBER_REF_6104 (pseudonymized)
  evidence_snapshot:
    PS-01: product_safety_profile_v12.3 [content_hash: bafybei...]
    PS-02: adverse_reaction_profile_v8.1 [content_hash: bafybei...]
    DS-01: contraindication_screening_output [content_hash: bafybei...]
```

```
    → result: ALERT_INTERACTION_MODERATE
    → interaction_database_version: IntDB-v2026.03
  DS-02: drug_interaction_screening_output [content_hash: bafybei...]
    → result: INTERACTION_DETECTED_MODERATE_SEVERITY
  DS-05: prescriber_clinical_rationale [content_hash: bafybei...]
    → rationale: "Patient has tolerated combination previously for
       18 months without adverse reaction; benefits outweigh risks
       in this clinical context"
algorithm_version: CDSS-v4.2.1
override_flag: true
override_justification: DS-05 reference above
review_posture: EXCEPTIONAL
content_address: bafybei_decision_state_07821...
```

Quality Review at T+6 months (Tier 1 Access):

Review Step	Action	Disclosure Level
1	Reviewer queries override frequency for CDSS-v4.2.1	Tier 0: aggregate statistics — "47 overrides in 6-month period; 12 for CONTRAINDICATION_OVERRIDE type"
2	Reviewer requests decision state records for CONTRAINDICATION_OVERRIDE events	Tier 1: decision state records with pseudonymized actor and patient; clinical rationale visible; interaction details visible; patient identity NOT disclosed
3	Reviewer verifies evidence snapshot currency: was IntDB-v2026.03 current at decision time?	Tier 1: version comparison — IntDB-v2026.03 was current at T+0; IntDB-v2026.09 is now current; reviewer checks whether new version would change the alert
4	Reviewer confirms override justification documentation adequate per Exceptional review posture requirements	Tier 1: DS-05 rationale reviewed; determination: "documentation adequate — prior tolerance history documented"
5	Post-access review completed; PARP generated	Independent reviewer: access scope verified; no escalation to Tier 2 required

Key Evidence Pattern: The reviewer reconstructed the complete decision context — what the CDSS showed, what the prescriber decided, what rationale was documented, and whether the evidence was current — without accessing patient identity, full clinical records, or the CDSS internal state. Bounded verification achieved.

15.5 Product Recall / Quarantine Workflow with Correction, Supersession, and Historical-State Preservation

Scenario. Manufacturer M issues a voluntary recall for Product W, Batch LOT-2026-0955, due to a confirmed potency deviation detected during stability testing. The recall affects an estimated 12,000 units distributed to 8 distributors and approximately 45 pharmacy/hospital endpoints.

Recall Lifecycle Summary:

Phase	Duration	Key Actions	Evidence Outputs
RECALL_INITIATED	T+0	Manufacturer M issues recall notification with scope: Product W, LOT-2026-0955, urgency classification = CLASS II (potential health impact, not immediately life-threatening)	Recall notification record (content-addressed); scope determination with aggregation hierarchy traversal; urgency classification documentation
RECALL_ACKNOWLEDGED	T+0 to T+48h	8 distributors and 45 endpoints receive notification; each acknowledges and reports affected inventory; total identified: 11,847 units (153 units already dispensed to patients)	53 CUS_RECALL_ACK events; inventory assessment records; 153 post-dispensation patient notification triggers
QUARANTINED	T+48h to T+72h	All 11,694 undispensed units quarantined at respective custody locations	45+ CUS_QUARANTINE_ENTRY events with segregation verification
RETURNED/DESTROYED	T+72h to T+30d	10,200 units returned to Manufacturer M; 1,494 units destroyed at custody locations (per institutional destruction policies)	CUS_RETURN events (return chain); CUS_DESTRUCTION events (witness records, disposal evidence)
Patient notification	T+48h to T+14d	153 patients notified per institutional policies; clinical assessment offered	Notification records (pseudonymized patient references); clinical re-assessment records where applicable
Scope correction	T+10d	Manufacturer M discovers additional 200 units from same batch shipped to 2 additional endpoints	Recall scope correction record (EP Delta): previous_scope → expanded_scope; additional notifications sent

Phase	Duration	Key Actions	Evidence Outputs
		not in original scope; recall scope expanded	
RECALL_CLOSED	T+45d	All 12,047 units accounted for: 10,400 returned, 1,494 destroyed, 153 dispensed (patients notified); open breaks = 0	Recall closure report: scope_total = 12,047; accounted = 12,047; unaccounted = 0; governance approval for closure

Historical-State Preservation: All pre-recall product states (PAES, CES, SES) are preserved in their original form. The recall does not overwrite or delete prior evidence. The recall events are additive — they extend the evidence chain. Post-recall, a reviewer can reconstruct both the pre-recall product state (what was known before the recall) and the recall lifecycle (how the recall was executed).

15.6 Optional Claim or Reimbursement Workflow Where Payout Progression Depends on Sufficient Evidence Linkage

Scenario. Pharmacy P submits a reimbursement claim (CLM-2026-08847) for the dispensation of Product V to Patient R. The benefit administrator's claim evidence gate detects that the authorization (prescription) referenced by the claim was revoked 3 days after dispensation. The revocation was due to the prescriber's credential restriction, not due to a problem with the dispensation itself.

Claim Lifecycle:

Time	Event	State	Evidence
T-10d	Prescription issued by Dr. K for Product V; dispensation executed at Pharmacy P; all gates passed at dispensation time	Authorization: VALID; Dispensation: RELEASED	AES (Dr. K legitimacy CONFIRMED at T-10d); dispensation evidence record with all gates PASS
T-7d	Dr. K's credential restricted (scope narrowed); prescription status unchanged in pharmacy system	Authorization: VALID (no revocation event yet for this specific prescription)	Dr. K credential restriction EP Delta
T-4d	Institutional governance reviews Dr. K's active prescriptions; revokes 12 prescriptions including Patient R's, effective immediately	Authorization: REVOKED	Revocation EP Delta for Patient R's prescription; downstream impact assessment: 1 dispensation already completed, 1 claim pending
T+0	Pharmacy P submits claim CLM-2026-08847	Claim: CLM_SUBMITTED	Claim record with dispensation reference, authorization reference
T+0:05	Claim evidence gate CG-2 (Authorization Linkage) evaluates:	Gate CG-2: PASS (temporal assessment)	Gate result: "Authorization REVOKED post-dispensation;

Time	Event	State	Evidence
	authorization is REVOKED — but temporal assessment confirms authorization was VALID at dispensation time (T-10d)		was VALID at dispensation time per temporal evidence assessment"
T+0:10	All claim evidence gates pass; claim validated	Claim: CLM_VALIDATED	Validation record with all gate results
T+1d	Claim adjudicated: approved for reimbursement; note attached that authorization was subsequently revoked but was valid at service time	Claim: CLM_APPROVED	Adjudication record with note referencing post-dispensation revocation
T+5d	Payout executed	Claim: CLM_PAID	Settlement confirmation

Key Evidence Pattern: The temporal evidence assessment (Section 12.2) evaluated authorization state at dispensation time, not at claim time. The post-dispensation revocation did not invalidate the claim because the dispensation was properly authorized when it occurred. The complete evidence chain — including the revocation and its timing — is preserved for reviewer access.

Appendix A — Product, Authorization, Custody, and Proof-of-Safety State Taxonomy Tables (Full)

A.1 Product Authenticity State — Complete Values

State Value	Code	Definition	Transition From	Transition To	Evidence Required
Verified	AUTH_VERIFIED	All authenticity evidence elements present, current, and consistent	NOT_ASSESSED, UNRESOLVED, RECONSTRUCTED (post-correction)	UNRESOLVED (evidence becomes stale), FAILED (contradiction detected)	Complete PAES; provenance manifest COMPLETE; manufacturer identity CONFIRMED; integrity checks PASS
Unresolved	AUTH_UNRESOLVED	Evidence incomplete, stale, or under investigation; no active contradiction	NOT_ASSESSED, AUTH_VERIFIED (if evidence becomes stale)	AUTH_VERIFIED (evidence completed/refreshed), FAILED (contradiction found)	Partial PAES with documented gaps; investigation ILS
Failed	AUTH_FAILED	Evidence actively contradicts claimed identity; counterfeit, substitution, or tampering indicator	AUTH_VERIFIED, AUTH_UNRESOLVED	QUARANTINE state in recall/hold taxonomy; RECONSTRUCTED (if investigation clears)	PAES with failure documentation; Preservation Bundle
Not Assessed	AUTH_NOT_ASSESSED	No authenticity verification performed	Initial state for newly received product	AUTH_VERIFIED, AUTH_UNRESOLVED, AUTH_FAILED	No PAES exists

A.2 Provenance State — Complete Values

State Value	Code	Definition	Evidence Required
Complete	PROV_COMPLETE	Full provenance chain documented; no gaps; all custody transitions evidenced	Content-addressed provenance manifest; all events hash-chained
Partial	PROV_PARTIAL	Documented segments present; at least one gap identified	Partial manifest with gap indicators; gap severity assessment
Broken	PROV_BROKEN	Confirmed break: custody transition with absent, contradictory, or tampered evidence	Break detection record; Preservation Bundle; hold-only triggered
Reconstructed	PROV_RECONSTRUCTED	Previous break resolved through investigation and compensating	Original break evidence preserved; reconstruction evidence with approval logs

State Value	Code	Definition	Evidence Required
		evidence	

A.3 Issuer / Prescriber / Authorizer Legitimacy State — Complete Values

State Value	Code	Definition	Freshness Requirement
Confirmed	ISSU_CONFIRMED	Authority verified; scope and jurisdiction validated; no revocation detected	Per authority type freshness window (Section 5.4)
Expired	ISSU_EXPIRED	Credentials or authority expired at or before relevant action	N/A (terminal state until renewal)
Revoked	ISSU_REVOKED	Authority revoked by credentialing body or governance process	N/A (terminal state; new credentialing required)
Restricted	ISSU_RESTRICTED	Authority held but with scope limitations affecting the specific action	Same freshness as CONFIRMED; restriction details verified at each use
Unverified	ISSU_UNVERIFIED	No verification performed or verification pending	Assessment required before downstream action

A.4 Prescription / Instruction Validity State — Complete Values

State Value	Code	Definition	Lifecycle Transitions
Valid	RX_VALID	Current, within scope, issued by confirmed authority, not superseded or revoked	→ EXPIRED (time), SUPERSEDED (replacement), REVOKED (explicit), SUSPENDED (investigation)
Expired	RX_EXPIRED	Validity window elapsed	Terminal unless renewed (→ RX_VALID via renewal event)
Superseded	RX_SUPERSEDED	Replaced by newer prescription for same scope	Terminal; pointer to superseding prescription maintained
Revoked	RX_REVOKED	Explicitly revoked by issuer, governance, or regulatory action	Terminal; new prescription required
Suspended	RX_SUSPENDED	Validity temporarily held pending investigation	→ RX_VALID (reinstated), RX_REVOKED (confirmed invalid)
Partial	RX_PARTIAL	Valid for some components but not all (e.g., product valid but refill count exhausted)	Component-level resolution required

A.5 Chain-of-Custody State — Complete Values

State Value	Code	Definition	Downstream Consequence
Intact	CUST_INTACT	Complete, unbroken chain; all handoffs documented and	Product eligible for dispensation (custody

State Value	Code	Definition	Downstream Consequence
		content-addressed	gate passes)
Gapped	CUST_GAPPED	One or more transitions lack evidence	Hold-only if gap exceeds materiality; assessment required
Compromised	CUST_COMPROMISED	Unauthorized custody event, storage violation, or tampering detected	Quarantine; incident escalation; Preservation Bundle
Reconstructed	CUST_RECONSTRUCTED	Previous gap resolved through investigation and compensating evidence	Gap evidence preserved; reconstruction documented with approval

A.6 Dispensation / Release State — Complete Values

State Value	Code	Definition	Prerequisites
Released	DISP_RELEASED	Product dispensed to intended recipient under documented conditions	All precondition gates passed; dispensation evidence record generated
Held	DISP_HELD	Product available but release blocked	At least one precondition gate failed or evidence state unresolved
Returned	DISP_RETURNED	Product returned by recipient; re-entered custody chain	Return event documented; product re-assessment triggered
Recalled	DISP_RECALLED	Product recalled from recipient	Recall event documented; acknowledgment and return/destruction tracked

A.7 Proof-of-Safety State — Complete Values

State Value	Code	Definition	Required Action
Sufficient	SAFE_SUFFICIENT	Required evidence classes present, current, and consistent	Standard or enhanced review posture per Section 7.4
Insufficient	SAFE_INSUFFICIENT	One or more required evidence classes missing, stale, or inconsistent	Dispensation blocked; evidence refresh or escalation required
Superseded	SAFE_SUPERSEDED	Previously sufficient evidence superseded by updated data	Re-assessment required before next dispensation
Disputed	SAFE_DISPUTED	Conflicting evidence classes without resolution documentation	Hold-only; reviewer access; clinical determination required

A.8 Product Recall / Quarantine / Hold State — Complete Values

State Value	Code	Definition	Governance
Active	HOLD_ACTIVE	Normal operational flow; no recall, quarantine, or hold	Standard reconciliation cadence

State Value	Code	Definition	Governance
Hold	HOLD_HELD	Hold-only containment pending investigation	Hold authority, scope, duration documented
Quarantined	HOLD_QUARANTINED	Physically or logically segregated from dispensable inventory	Quarantine reason, authority, release conditions documented
Recalled	HOLD_RECALLED	Subject to recall; downstream holders notified	Recall scope, acknowledgment tracking, return/destruction evidence
Withdrawn	HOLD_WITHDRAWN	Permanently removed from supply chain	Withdrawal authority; disposal documentation
Released from Hold	HOLD_RELEASED	Previously held; released after resolution	Resolution evidence, approval chain, post-release verification

A.9 Correction / Supersession / Revocation State — Complete Values

State Value	Code	Definition	Preservation Rule
Current	CORR_CURRENT	Active, authoritative version	Standard reconciliation
Corrected	CORR_CORRECTED	Correction applied; corrected version is now CURRENT	Prior version retained; EP Delta generated
Superseded	CORR_SUPERSEDED	Newer version replaces this one	Supersession chain maintained; prior preserved
Revoked	CORR_REVOKED	Invalidated; may not be relied upon for new actions	Revocation record; propagation to dependents

A.10 Claim / Reimbursement / Settlement State — Complete Values (Optional)

State Value	Code	Definition	Evidence Linkage
Submitted	CLM_SUBMITTED	Claim submitted for adjudication	Linked to dispensation, authorization, product evidence
Validated	CLM_VALIDATED	Evidence gates passed	Validation record with gate results
Adjudicated	CLM_ADJUDICATED	Determination issued	Adjudication record with reviewed evidence
Approved	CLM_APPROVED	Approved for payout	Evidence sufficiency confirmation
Denied	CLM_DENIED	Denied with documented reason	Denial record with reason and appeal pathway
Paid	CLM_PAID	Payout executed and confirmed	Settlement confirmation with payment reference
Held	CLM_HELD	Progression suspended	Hold reason; linked evidence state unresolved
Adjusted	CLM_ADJUSTED	Post-payment correction	Adjustment record with reason and evidence rebinding
Reversed	CLM_REVERSED	Full reversal	Reversal record with recovery initiation
Appealed	CLM_APPEALED	Denial or adjustment appealed	Appeal submission with additional evidence

Appendix B — Evidence Set Mapping Templates for Product, Prescription, Custody, Review, and Claim States

B.1 Product Authenticity Evidence Set (PAES) — Mapping Template

Purpose. Maps the evidence artifacts required to support each product authenticity state value. For each state, the template identifies the required evidence elements, their sources, content-addressing requirements, and linkage to other evidence sets.

PAES Mapping Matrix:

Evidence Element	Required for VERIFIED	Required for UNRESOLVED	Content-Addressed	Source System	Linked Evidence Sets
Canonical Product Object (CPO)	Yes — complete, integrity-verified	Yes — must exist even if other elements incomplete	Yes	Manufacturer or product registry	CES (product reference); AES (manufacturer credential)
Manufacturer identity credential reference	Yes — ISSU_CONFIRMED within freshness	Optional (verification may be pending)	Yes	Credentialing body via AES	AES (issuer legitimacy)
Batch/lot release documentation	Yes — complete	Optional (may be the missing element)	Yes	Manufacturer production records	CES (custody chain origin)
Provenance manifest	Yes — PROV_COMPLETE	Yes — PROV_PARTIAL acceptable with gap documentation	Yes	Aggregated from custody events	CES (custody event chain)
Most recent custody handoff confirmation	Yes — within freshness	Optional (may be stale)	Yes	Current custodian	CES (most recent custody event)
Content-addressed integrity verification	Yes — PASS	Yes — must be attempted	Yes	Hash verification process	All linked evidence sets

PAES Manifest Template (Conceptual):

```
paes_manifest:
  manifest_id: [content_address]
  pack_type: PAES
  product_reference:
    cpo_content_address: [hash]
    product_reference_id: [identifier]
    batch_lot_reference: [identifier]
  authenticity_state: VERIFIED | UNRESOLVED | FAILED | NOT_ASSESSED
  state_determination_timestamp: [UTC]
  evidence_inventory:
```

```
  cpo:
    content_address: [hash]
    integrity_status: PASS | FAIL
  manufacturer_credential:
    aes_reference: [content_address of AES]
    legitimacy_state: [ISSU_ value]
    freshness_status: CURRENT | EXPIRING | EXPIRED
  batch_lot_documentation:
    content_address: [hash]
    present: true | false
  provenance_manifest:
    content_address: [hash]
    chain_status: COMPLETE | PARTIAL | BROKEN
  most_recent_custody_event:
    content_address: [hash]
    event_type: [CUS_ code]
    event_timestamp: [UTC]
    freshness_status: CURRENT | STALE
  integrity_verification:
    verification_timestamp: [UTC]
    result: PASS | FAIL
gap_documentation:
  - element: [name of missing/stale element]
    reason: [reason code]
    investigation_reference: [ILS pointer if under investigation]
linked_evidence_sets:
  aes_references: [list of content addresses]
  ces_references: [list of content addresses]
  ses_references: [list of content addresses]
manifest_content_address: [self-referential hash]
```

B.2 Authorization Evidence Set (AES) — Mapping Template

Purpose. Maps the evidence artifacts required to support each authorization and issuer legitimacy state value.

AES Mapping Matrix:

Evidence Element	Required for ISSU_CONFIRMED	Required for RX_VALID	Content-Addressed	Source System	Linked Evidence Sets
Issuer credential reference	Yes — active, non-revoked	Yes (via AES linkage)	Yes	Credentialing body or institutional records	PAES (manufacturer identity for product-level auth)
Scope attestation	Yes — covering the specific action	Yes — scope matches dispensation parameters	Yes	Credential content or institutional records	DEP-H (dispensation scope match)
Currency check record	Yes — within freshness window	Yes (implied by ISSU_CONFIRMED)	Yes	Verification process output	—
Revocation check result	Yes — CLEAR	Yes (implied by ISSU_CONFIRMED)	Yes	Revocation list or status registry	—
Prescription record (for RX states)	N/A (issuer-level)	Yes — complete with all bound fields	Yes	Prescribing system	DEP-H (authorization linkage)
Supersession chain (if applicable)	N/A	Yes — current-reference state determined	Yes	Supersession chain records	Prior AES versions (historical)
Delegation record (if delegated)	Yes — delegation instrument current	Yes — delegator AES confirmed	Yes	Institutional records	Delegator AES

AES Manifest Template (Conceptual):

```
aes_manifest:
  manifest_id: [content_address]
  pack_type: AES
  authorization_reference:
    authorization_id: [identifier]
    authorization_type: PRESCRIPTION | INSTITUTIONAL_ORDER |
                        STANDING_ORDER | EMERGENCY | DELEGATION
  issuer_legitimacy_state: [ISSU_ value]
  prescription_validity_state: [RX_ value] (if applicable)
  state_determination_timestamp: [UTC]
  evidence_inventory:
    issuer_credential:
      credential_reference: [content_address]
      authority_type: [prescribing | dispensing | delegating | recalling]
      scope_attestation: [content_address]
    currency_check:
```

```
    check_timestamp: [UTC]
    freshness_status: CURRENT | EXPIRING | EXPIRED
  revocation_check:
    check_timestamp: [UTC]
    result: CLEAR | REVOKED | RESTRICTED | UNAVAILABLE
    revocation_list_version: [reference]
  prescription_record: (if applicable)
    content_address: [hash]
    bounds:
      time_bound: {validity_start, validity_end}
      location_bound: {authorized_locations[]}
      quantity_bound: {max_quantity, dispensed_to_date}
      product_bound: {authorized_products[]}
  supersession_chain: (if applicable)
    chain_id: [content_address]
    current_reference: [content_address of current version]
    version_count: [integer]
  delegation_record: (if delegated)
    delegation_instrument: [content_address]
    delegator_aes_reference: [content_address]
    delegation_scope: [scope description]
    delegation_validity: {start, end}
linked_evidence_sets:
  paes_references: [list — product-level authorization]
  dep_h_references: [list — dispensation linkage]
manifest_content_address: [self-referential hash]
```

B.3 Custody Evidence Set (CES) — Mapping Template

Purpose. Maps the evidence artifacts required to support each chain-of-custody state value.

CES Mapping Matrix:

Evidence Element	Required for CUST_INTACT	Required for CUST_GAPPED	Content-Addressed	Source System	Linked Evidence Sets
Complete custody event chain	Yes — all events from entry to current position, hash-chained	Partial — chain present but with documented gaps	Yes	Custody event logging systems	PAES (provenance manifest cross-reference)

Evidence Element	Required for CUST_INTACT	Required for CUST_GAPPED	Content-Addressed	Source System	Linked Evidence Sets
Handoff confirmations (sender + receiver)	Yes — matched pairs for all transitions	Yes — present for documented segments; gaps indicated	Yes	Transferring and receiving entities	—
Storage condition logs	Yes — continuous for all storage periods	Yes — present for documented storage periods	Yes	Storage monitoring systems	SES (PS-03 storage condition compliance)
Excursion records and assessments	Yes — all excursions documented and assessed	Yes — excursions in documented periods assessed	Yes	Monitoring systems + quality assessors	SES (PS-04 product integrity)
Repackaging records (if applicable)	Yes — with authorized repackager credential	If present in documented segments	Yes	Repackaging entity	PAES (aggregation hierarchy)
Current custodian verification	Yes — current holder confirmed	Yes — last known custodian documented	Yes	Current custodian	—

CES Manifest Template (Conceptual):

```
ces_manifest:
  manifest_id: [content_address]
  pack_type: CES
  product_reference:
    cpo_content_address: [hash]
    aggregation_level: UNIT | PACKAGE | CASE | PALLET | BATCH
  custody_state: CUST_INTACT | CUST_GAPPED | CUST_COMPROMISED |
                 CUST_RECONSTRUCTED
  state_determination_timestamp: [UTC]
  chain_summary:
    first_event_hash: [hash of genesis custody event]
    last_event_hash: [hash of most recent event]
    event_count: [integer]
    gap_count: [integer — 0 for INTACT]
    excursion_count: [integer]
    excursions_assessed: [integer — must equal excursion_count for INTACT]
  evidence_inventory:
    custody_events:
```

```
    - event_hash: [content_address]
      event_type: [CUS_ code]
      event_timestamp: [UTC]
      actor_id: [pseudonymized]
      chain_integrity: VALID | BREAK
  storage_condition_logs:
    - storage_period_id: [identifier]
      facility_reference: [pseudonymized]
      condition_log_hash: [content_address]
      excursion_records: [list of content addresses]
  handoff_pairs:
    - handoff_hash: [content_address]
      receipt_hash: [content_address]
      matched: true | false
gap_documentation: (if GAPPED)
  - gap_start_event: [last known event before gap]
    gap_end_event: [first known event after gap]
    gap_duration: [duration]
    severity_assessment: [SEV-1 through SEV-4]
    investigation_reference: [ILS pointer]
linked_evidence_sets:
  paes_reference: [content_address — provenance manifest alignment]
  ses_references: [list — storage condition linkage to safety evidence]
manifest_content_address: [self-referential hash]
```

B.4 Safety Evidence Set (SES) — Mapping Template

Purpose. Maps the evidence artifacts required to support each proof-of-safety state value.

SES Mapping Matrix:

Evidence Element	Required for SAFE_SUFFICIENT (Standard)	Required for SAFE_SUFFICIENT (High-Impact)	Content-Addressed	Source System
PS-01: Product safety profile reference	Yes	Yes	Yes	Manufacturer / product registry
PS-02: Known adverse reaction profile	No (standard)	Yes	Yes	Manufacturer safety communications

Evidence Element	Required for SAFE_SUFFICIENT (Standard)	Required for SAFE_SUFFICIENT (High-Impact)	Content-Addressed	Source System
PS-03: Storage condition compliance	Yes	Yes	Yes	CES storage condition logs
PS-04: Product integrity confirmation	Yes	Yes	Yes	CES receipt and dispensation records
PS-05: Recall/withdrawal status	Yes	Yes	Yes	Recall status registry
DS-01: Contraindication screening output	Yes	Yes	Yes	Clinical decision-support system
DS-02: Drug interaction screening output	Yes	Yes	Yes	Clinical decision-support system
DS-03: Dosage/quantity appropriateness	Yes	Yes	Yes	Dispensing system / pharmacist
DS-04: Clinical decision-support output	No (standard)	Yes (high-impact)	Yes	Clinical decision-support system
DS-05: Prescriber clinical rationale	No (standard, unless override)	Yes (if override)	Yes	Prescriber documentation

SES Manifest Template (Conceptual):

```
ses_manifest:
  manifest_id: [content_address]
  pack_type: SES
  subject_reference:
    product_cpo: [content_address]
    dispensation_event: [content_address] (if dispensation-specific)
    decision_state: [content_address] (if decision-specific)
  safety_state: SAFE_SUFFICIENT | SAFE_INSUFFICIENT | SAFE_SUPERSEDED |
                SAFE_DISPUTED
  review_posture: STANDARD | ENHANCED | EXCEPTIONAL
  state_determination_timestamp: [UTC]
  evidence_inventory:
    product_level:
      PS-01: {content_address, version, freshness_status}
      PS-02: {content_address, version, freshness_status}  # null if not
required
```

```
      PS-03: {ces_reference, storage_compliance_status}
      PS-04: {ces_reference, integrity_status}
      PS-05: {recall_status_check_timestamp, result}
    decision_level:
      DS-01: {content_address, database_version, result, freshness_status}
      DS-02: {content_address, database_version, result, freshness_status}
      DS-03: {content_address, verification_result}
      DS-04: {content_address, algorithm_version, result}  # null if not
required
      DS-05: {content_address, rationale_summary}  # null if no override
  completeness_assessment:
    required_classes: [list per action type from Section 7.2]
    present_classes: [list of classes with evidence]
    missing_classes: [list of classes without evidence — drives INSUFFICIENT]
    stale_classes: [list of classes with expired freshness]
  context_bound_decision_states: (if applicable)
    - decision_id: [content_address]
      decision_type: [type code]
      override_flag: [boolean]
      review_posture: [STANDARD | ENHANCED | EXCEPTIONAL]
  linked_evidence_sets:
    paes_reference: [content_address — product identity linkage]
    aes_reference: [content_address — authorization linkage]
    ces_reference: [content_address — custody/storage linkage]
  manifest_content_address: [self-referential hash]
```

B.5 Dispensation Evidence Pack (DEP-H) — Mapping Template

Purpose. Maps the evidence artifacts produced at dispensation, linking all upstream evidence sets to the dispensation event.

DEP-H Mapping Matrix:

Evidence Element	Required	Content-Addressed	Source	Cross-Reference
Dispensation event record	Yes	Yes	Dispensing entity	CES (terminal custody event)
Precondition gate completion record	Yes — all gates G1–G7 with results	Yes	Gate evaluation engine	PAES (G1), AES (G2), scope match (G3), CES (G4), SES (G5), hold status (G6),

Evidence Element	Required	Content-Addressed	Source	Cross-Reference
				revocation (G7)
Dispensing entity credential	Yes	Yes	Dispensing entity AES	—
Recipient reference	Yes — pseudonymized per institutional policy	Yes	Dispensing entity	—
Authorization reference	Yes — pointer to AES with temporal validity confirmation	Yes	Prescribing system via AES	AES (authorization evidence)
Product reference	Yes — pointer to PAES with authenticity state	Yes	Product registry via PAES	PAES (product authenticity)
Safety evidence reference	Yes — pointer to SES with safety state	Yes	Clinical systems via SES	SES (proof-of-safety)

DEP-H Manifest Template (Conceptual):

```
dep_h_manifest:
  manifest_id: [content_address]
  pack_type: DEP-H
  dispensation_event:
    event_id: [content_address]
    event_timestamp: [UTC]
    dispensing_entity: [pseudonymized]
    recipient_reference: [pseudonymized]
  gate_completion:
    G1_product_authenticity: {result: PASS|FAIL, paes_ref: [hash]}
    G2_authorization_validity: {result: PASS|FAIL, aes_ref: [hash]}
    G3_scope_match: {result: PASS|FAIL, verification_ref: [hash]}
    G4_custody_integrity: {result: PASS|FAIL, ces_ref: [hash]}
    G5_safety_evidence: {result: PASS|FAIL, ses_ref: [hash]}
    G6_no_active_hold: {result: PASS|FAIL, hold_status_ref: [hash]}
    G7_revocation_check: {result: PASS|FAIL|N/A, vop_ref: [hash]}
  linked_evidence_sets:
    paes: [content_address]
    aes: [content_address]
    ces: [content_address]
    ses: [content_address]
  review_posture: STANDARD | ENHANCED | EXCEPTIONAL
```

```
  manifest_content_address: [self-referential hash]
```

B.6 Claim / Reimbursement Evidence Pack (CLM-EP) — Mapping Template (Optional)

Purpose. Maps the evidence artifacts required to support each claim/reimbursement state value. Included only where Section 12 is in scope.

CLM-EP Mapping Matrix:

Evidence Element	Required for CLM_APPROVED	Content-Addressed	Source	Cross-Reference
Claim submission record	Yes	Yes	Claimant / pharmacy	DEP-H (dispensation reference)
Claim evidence gate results (CG-1 through CG-6)	Yes — all gates passed	Yes	Benefit administrator gate engine	DEP-H, PAES, AES, CES, SES
Adjudication record	Yes — with determination and evidence references	Yes	Benefit administrator	—
Approval record	Yes — with evidence sufficiency confirmation	Yes	Benefit administrator	—
Payout execution confirmation	Yes (for CLM_PAID)	Yes	Payment system	—
Temporal evidence assessment	Yes — confirming authorization valid at dispensation time	Yes	Gate engine temporal logic	AES (authorization timeline)
Linked dispensation evidence	Yes — DEP-H reference	Yes	DEP-H	All upstream evidence sets via DEP-H

CLM-EP Manifest Template (Conceptual):

```
clm_ep_manifest:
  manifest_id: [content_address]
  pack_type: CLM-EP
  claim_reference:
    claim_id: [identifier]
    claim_status: [CLM_ value]
  dispensation_reference:
    dep_h_manifest: [content_address]
    dispensation_timestamp: [UTC]
  evidence_gates:
    CG-1: {result, dispensation_evidence_ref}
    CG-2: {result, authorization_temporal_assessment}
```

```
  CG-3: {result, authenticity_state_at_dispensation}
  CG-4: {result, safety_state_at_dispensation}
  CG-5: {result, recall_status_at_submission}
  CG-6: {result, duplicate_check_ref}
adjudication:
  adjudication_record: [content_address]
  determination: APPROVED | DENIED | PENDED
  reason_code: [code]
payout: (if CLM_PAID)
  payment_reference: [identifier]
  amount: [value]
  execution_timestamp: [UTC]
  settlement_status: SETTLED | FAILED
open_breaks: [count of unresolved breaks for this claim]
linked_evidence_sets:
  paes: [content_address via DEP-H]
  aes: [content_address via DEP-H]
  ces: [content_address via DEP-H]
  ses: [content_address via DEP-H]
manifest_content_address: [self-referential hash]
```

Appendix C — Reconciliation Break Taxonomy for Authenticity, Provenance, Custody, and Safety Workflows

C.1 Purpose and Scope

This appendix provides the complete reconciliation break taxonomy referenced throughout the framework. Each break type is defined with detection criteria, severity classification logic, default containment response, resolution pathway, and evidence requirements. The taxonomy extends Baseline A's reconciliation break classification to healthcare product, authorization, custody, and safety evidence domains.

Taxonomy Conventions:

- Break codes use the prefix BRK- followed by a domain identifier (PROV, AUTH, CUST, SAFE, CLAIM, INTEG, FRESH).
- Each break type may manifest at multiple severity levels depending on context (product category, operational phase, recurrence pattern).
- Severity is assessed at detection using the criteria in this appendix; severity may be escalated during investigation if aggravating factors emerge.
- All break records are ILS entries with content-addressed integrity, linked to the reconciliation execution that detected them.

C.2 Provenance Break Taxonomy (BRK-PROV)

Break Code	Break Name	Detection Criteria	Default Severity	Containment Response
BRK-PROV-001	Custody gap — missing handoff record	Provenance manifest shows event chain discontinuity; expected CUS_HANDOFF absent between two custody nodes	SEV-2 (High) for narrow therapeutic index / controlled substances; SEV-3 (Moderate) for standard products	Hold-only containment on affected units; investigation of gap period
BRK-PROV-002	Provenance chain hash break	Content-addressed hash verification fails at one or more event transitions in the provenance manifest	SEV-1 (Critical) — potential tampering	Immediate hold; quarantine assessment; incident escalation; Preservation Bundle
BRK-PROV-003	Manufacturer identity mismatch	CPO manufacturer_id does not match the manufacturer credential presented in the PAES; or manufacturer credential fails verification	SEV-1 (Critical) — potential counterfeit	Immediate hold; quarantine; counterfeit investigation protocol; regulatory notification per institutional policy
BRK-PROV-004	Batch/lot reference discrepancy	Physical product batch/lot reference does not match the provenance manifest	SEV-2 (High)	Hold-only containment; manufacturer investigation; may resolve as labeling error (see worked example 15.1) or

Break Code	Break Name	Detection Criteria	Default Severity	Containment Response
		batch/lot reference (labeling vs. electronic record)		escalate to counterfeit investigation
BRK-PROV-005	Duplicate unit identifier	Two or more distinct products in the custody chain claim the same unit-level identifier (serial number collision)	SEV-1 (Critical) — potential counterfeit or system error	Immediate hold on all units claiming the identifier; incident investigation; regulatory notification if counterfeit suspected
BRK-PROV-006	Aggregation hierarchy break	Child product unit cannot be traced to parent aggregation level (package, case, pallet) through content-addressed linkage	SEV-3 (Moderate) if isolated; SEV-2 if pattern affects multiple units	Hold-only on affected units; aggregation chain investigation; potential repackaging authority review
BRK-PROV-007	Provenance manifest unavailable	Content-addressed provenance manifest cannot be retrieved from storage for a product requiring authenticity verification	SEV-2 (High)	Hold-only containment; storage availability incident; recovery from replicated storage per Baseline C procedures
BRK-PROV-008	Storage condition gap in provenance	Provenance chain shows a storage period without corresponding condition monitoring records	SEV-3 (Moderate) if short gap and standard product; SEV-2 if cold-chain product or extended gap	Hold-only if product is condition-sensitive; storage evidence refresh required before release

Provenance Break Resolution Pathways:

Resolution Type	Applicable Break Codes	Resolution Evidence	Post-Resolution State
Manufacturer correction (labeling / documentation error)	BRK-PROV-004	Manufacturer correction attestation; corrected documentation; quality assessment confirming no product impact	PROV_RECONSTRUCTED; EP Delta generated
Gap investigation — compensating evidence obtained	BRK-PROV-001, BRK-PROV-008	Investigation report; compensating evidence (transport records, third-party attestation, retrospective condition data)	PROV_RECONSTRUCTED; gap documented with compensating evidence
Counterfeit confirmed	BRK-PROV-003, BRK-PROV-005	Investigation report confirming counterfeit; regulatory notification record; quarantine/destruction evidence	AUTH_FAILED; product removed from supply chain; Preservation Bundle sealed

Resolution Type	Applicable Break Codes	Resolution Evidence	Post-Resolution State
Storage recovery — manifest restored	BRK-PROV-007	Storage recovery log; restored manifest integrity verification; availability incident investigation	PROV state restored to pre-incident value; availability incident documented
Integrity failure — tampered record identified	BRK-PROV-002	Forensic investigation report; valid version restoration from backup; tamper evidence preserved	PROV_RECONSTRUCTED if valid version exists; escalation to governance if unrecoverable

---

C.3 Authorization Break Taxonomy (BRK-AUTH)

Break Code	Break Name	Detection Criteria	Default Severity	Containment Response
BRK-AUTH-001	Dispensation bound to expired authorization	Reconciliation detects a completed or pending dispensation event referencing an authorization whose validity state = RX_EXPIRED at dispensation time	SEV-2 (High) if dispensation already completed; SEV-3 if dispensation pending (can be corrected)	Pending dispensation: hold. Completed dispensation: post-dispensation review; patient notification assessment
BRK-AUTH-002	Dispensation bound to revoked authorization	Dispensation references an authorization with validity state = RX_REVOKED; revocation preceded dispensation	SEV-1 (Critical)	Immediate investigation; patient safety assessment; incident escalation; Preservation Bundle
BRK-AUTH-003	Issuer credential expired at authorization time	AES shows issuer legitimacy = ISSU_EXPIRED at the timestamp of the authorization event	SEV-2 (High)	Hold on pending dispensation under affected authorization; investigation of authorization validity
BRK-AUTH-004	Issuer credential revoked — active prescriptions outstanding	Credentialing body revokes issuer; reconciliation identifies active (non-expired, non-superseded) prescriptions from revoked issuer	SEV-2 (High)	All active prescriptions flagged for review; pending dispensation held; institutional process for prescription transfer or re-authorization
BRK-AUTH-005	Scope mismatch — authorization bounds exceeded	Dispensation parameters (product, quantity, location, purpose) do not match authorization bounds documented in AES	SEV-2 (High) if material mismatch; SEV-3 if minor (e.g., dispensation location different from authorized but within same institution)	Hold on dispensation; scope-match investigation; may resolve with documented override or escalate as unauthorized dispensation
BRK-AUTH-006	Supersession chain ambiguity	Multiple prescriptions for the same scope claim	SEV-2 (High)	Hold on all affected prescriptions; Tier 1

Break Code	Break Name	Detection Criteria	Default Severity	Containment Response
		RX_VALID status; current-reference state cannot be determined from the supersession chain		supersession chain review; determination of authoritative current-reference
BRK-AUTH-007	Delegation instrument expired or revoked	Dispensation executed under delegated authority; delegation instrument expired or delegator AES shows revocation at delegation time	SEV-2 (High)	Post-dispensation review for completed events; hold on future delegated actions pending delegation renewal
BRK-AUTH-008	Authorization freshness exceeded	AES currency_check_timestamp exceeds the applicable freshness window for the authority type; dispensation proceeds on stale verification	SEV-3 (Moderate) if freshness exceeded by <50% of window; SEV-2 if exceeded by >50%	Re-verification required before next dispensation; investigation of freshness monitoring process

Authorization Break Resolution Pathways:

Resolution Type	Applicable Break Codes	Resolution Evidence	Post-Resolution State
Re-authorization by same or substitute issuer	BRK-AUTH-001, BRK-AUTH-003, BRK-AUTH-004, BRK-AUTH-007	New authorization or renewal issued by authorized issuer; AES confirmed for new authorization	Pending dispensation proceeds under new authorization; EP Delta documenting break and re-authorization
Scope correction	BRK-AUTH-005	Scope verification identifies error in dispensation parameters or authorization bounds; correction EP Delta generated	Authorization confirmed valid with corrected scope documentation
Supersession chain repair	BRK-AUTH-006	Investigation determines correct current-reference; EP Delta resolves ambiguity; non-current prescriptions marked SUPERSEDED	Single current-reference state established; hold released
Unauthorized dispensation confirmed	BRK-AUTH-002	Investigation confirms dispensation occurred under revoked authorization; patient safety assessment; institutional corrective action	Preservation Bundle sealed; liability trigger event documented; corrective action per institutional governance

C.4 Custody Break Taxonomy (BRK-CUST)

Break Code	Break Name	Detection Criteria	Default Severity	Containment Response
BRK-CUST-001	Unmatched handoff	CUS_HANDOFF record exists	SEV-2 (High)	Hold-only on affected

Break Code	Break Name	Detection Criteria	Default Severity	Containment Response
	— sender confirms, receiver does not	but no matching CUS_RECEIPT within expected timeframe	— product location uncertain	units; investigation of receiving entity; transport chain review
BRK-CUST-002	Unauthorized custody event — unrecognized actor	Custody event logged by actor whose credential cannot be verified against authorized custodian registry	SEV-1 (Critical)	Immediate hold; incident escalation; Preservation Bundle; potential unauthorized access investigation
BRK-CUST-003	Storage excursion unassessed	CUS_TEMP_EXCURSION event logged without corresponding excursion assessment record within SLA	SEV-3 (Moderate) for minor excursion; SEV-2 for moderate or severe excursion	Hold-only until excursion assessment completed; product quality review
BRK-CUST-004	Quantity discrepancy at handoff	CUS_RECEIPT quantity does not match CUS_HANDOFF quantity for the same transfer	SEV-3 if <1% variance; SEV-2 if 1–5% variance; SEV-1 if >5% variance	Investigation of discrepancy; transport chain review; potential loss or diversion assessment
BRK-CUST-005	Product identity mismatch at receipt	CUS_RECEIPT product verification shows CPO mismatch with handoff documentation	SEV-1 (Critical) — potential substitution	Immediate hold; return to sender or quarantine; counterfeit/substitution investigation
BRK-CUST-006	Custody chain exceeds maximum age without refresh	Most recent custody event for product exceeds the freshness threshold for the product category without a new event	SEV-3 (Moderate) if within 2x threshold; SEV-2 if beyond 2x threshold	Re-verification required; manual custody confirmation per Section 6.4
BRK-CUST-007	Repackaging without authorized entity credential	CUS_REPACKAGE event logged by entity without documented repackaging authorization	SEV-2 (High)	Hold on repackaged units; repackaging authority investigation; potential product integrity assessment
BRK-CUST-008	Recall acknowledgment overdue	CUS_RECALL_ACK not received from notified custody holder within recall acknowledgment SLA	SEV-2 (High) — recalled product may remain in dispensable inventory	Escalation to recall authority; direct outreach to custody holder; regulatory notification if SLA significantly exceeded

C.5 Safety Evidence Break Taxonomy (BRK-SAFE)

Break Code	Break Name	Detection Criteria	Default Severity	Containment Response
BRK-SAFE-001	Required evidence class absent at dispensation	Dispensation completed without one or more required safety evidence classes per Section 7.2 matrix	SEV-2 (High) for high-impact classes (DS-01, DS-02); SEV-3 for supplementary classes	Post-dispensation review for completed events; hold on future dispensation until evidence generated
BRK-SAFE-002	Safety evidence stale at dispensation	Safety evidence class generated against a source data version that was superseded before dispensation occurred	SEV-3 (Moderate) if supersession is minor update; SEV-2 if supersession involves new safety information	Re-assessment required before next dispensation; investigation of freshness monitoring
BRK-SAFE-003	Safety alert overridden without documentation	SAFETY_ALERT_OVERRIDDEN event without corresponding DS-05 (prescriber clinical rationale) evidence	SEV-2 (High) — accountability gap	Post-dispensation review; retrospective DS-05 documentation required; institutional governance notification
BRK-SAFE-004	Decision-support algorithm version deprecated	Context-bound decision state references a CDSS algorithm version that has been deprecated or recalled by the system vendor	SEV-3 (Moderate) if deprecated version produces equivalent results; SEV-2 if deprecated due to known error	Inventory of decisions relying on deprecated version; assessment of whether version change affects clinical outputs
BRK-SAFE-005	Conflicting safety evidence classes	Two or more safety evidence classes produce contradictory assessments (e.g., DS-01 flags contraindication; dispensation proceeds without override documentation)	SEV-2 (High)	SAFE_DISPUTED state triggered; hold on future dispensation; clinical review required
BRK-SAFE-006	Product safety profile updated post-dispensation — pre-refill	Manufacturer issues safety update for product; active prescriptions exist for the product; next refill has not yet incorporated updated safety information	SEV-3 (Moderate)	Prescriber notification required; refill blocked until SES refreshed with updated PS-01/PS-02

C.6 Claim / Reimbursement Break Taxonomy (BRK-CLAIM) — Optional

Included only where Section 12 is in scope.

Break Code	Break Name	Detection Criteria	Default Severity	Containment Response
BRK-CLAIM-001	Claim without dispensation evidence	CLM_SUBMITTED references a dispensation event for which no DEP-H exists	SEV-2 (High)	Claim pended (CLM_PENDED); dispensation evidence investigation

Break Code	Break Name	Detection Criteria	Default Severity	Containment Response
		or the DEP-H is integrity-failed		
BRK-CLAIM-002	Claim references revoked authorization (pre-dispensation)	CLM_SUBMITTED references an authorization that was RX_REVOKED before the dispensation event occurred	SEV-1 (Critical) — unauthorized dispensation may have occurred	Claim denied; dispensation investigation; patient safety assessment; Preservation Bundle
BRK-CLAIM-003	Duplicate claim detected	Two claims reference the same dispensation event with overlapping coverage	SEV-2 (High)	Both claims held; investigation of duplication source
BRK-CLAIM-004	Payout without approved claim	Payment system records a payout without a corresponding CLM_APPROVED record	SEV-1 (Critical) — potential unauthorized payment	Immediate investigation; recovery assessment; system control review
BRK-CLAIM-005	Payout amount mismatch	CLM_PAID amount differs from CLM_APPROVED amount beyond defined tolerance	SEV-3 if within rounding tolerance; SEV-2 if material	Adjustment (CLM_ADJUSTED) for amount correction; investigation for systemic pricing errors
BRK-CLAIM-006	Orphaned adjustment	CLM_ADJUSTED record exists without corresponding original CLM_PAID	SEV-2 (High)	Investigation of adjustment origin; correction or reversal per determination

---

C.7 Integrity Break Taxonomy (BRK-INTEG)

Break Code	Break Name	Detection Criteria	Default Severity	Containment Response
BRK-INTEG-001	Content-address verification failure	Computed hash of retrieved artifact does not match stored content address	SEV-1 (Critical) — potential tampering or corruption	Immediate hold on dependent states; artifact recovery from replicated storage; forensic investigation
BRK-INTEG-002	Hash chain break in event sequence	Previous_event_hash in an event record does not match the content_address of the preceding event	SEV-1 (Critical) — potential insertion, deletion, or reordering	Immediate hold on affected chain; forensic investigation; Preservation Bundle
BRK-INTEG-003	Evidence artifact unavailable	Content-addressed artifact referenced by a manifest cannot be retrieved from any storage replica	SEV-2 (High)	Hold on dependent states; storage recovery procedures; evidence gap documented if unrecoverable

Break Code	Break Name	Detection Criteria	Default Severity	Containment Response
BRK-INTEG-004	Manifest self-referential hash failure	Evidence pack manifest's computed hash does not match its declared manifest_content_address	SEV-1 (Critical)	Manifest quarantined; all artifacts within the manifest re-verified individually; investigation of manifest corruption source
BRK-INTEG-005	Silent overwrite detected	Evidence artifact modified after storage without generating a correction EP Delta; detected through periodic hash verification or audit	SEV-1 (Critical) — governance violation	Immediate governance notification; liability trigger event LT-07; forensic investigation of modification source and scope

---

C.8 Freshness Break Taxonomy (BRK-FRESH)

Break Code	Break Name	Detection Criteria	Default Severity	Containment Response
BRK-FRESH-001	Issuer credential verification stale	AES currency_check_timestamp exceeds freshness window for the authority type	SEV-3 (Moderate) if <50% beyond window; SEV-2 if >50%	Re-verification required before next downstream action
BRK-FRESH-002	Safety evidence source data outdated	Safety evidence class generated against source data version that has been superseded by a material update	SEV-3 or SEV-2 depending on materiality of update	Evidence refresh required; SES state may transition to SAFE_SUPERSEDED
BRK-FRESH-003	Custody evidence stale	Most recent custody event exceeds product-category freshness threshold	SEV-3 if <2x threshold; SEV-2 if >2x	Manual custody re-verification required (Section 6.4 manual confirmation pathway)
BRK-FRESH-004	Revocation check stale	Revocation check result was obtained beyond the acceptable freshness window for the transaction type	SEV-3 (Moderate); SEV-2 for high-risk transactions	Re-check required before relying on prior result; conservative FAIL treatment per Baseline D
BRK-FRESH-005	Reconciliation execution overdue	Reconciliation cycle not executed within the defined cadence for the reconciliation type	SEV-3 if one cycle missed; SEV-2 if two or more consecutive cycles missed	Reconciliation execution required; investigation of monitoring process; governance notification if pattern persists

---

C.9 Severity Assessment Decision Logic

When a break is detected, severity is assessed using the following decision tree:

```
Step 1: Identify break code from taxonomy (C.2 through C.8)
```

```
Step 2: Assess base severity from taxonomy table

Step 3: Apply aggravating factors (each may escalate severity by one level):
  - Product is narrow therapeutic index, biologic, or controlled substance
  - Break affects multiple products or multiple custody holders
  - Break is recurrent (same break code detected 3+ times in 30 days
    for the same scope)
  - Break was not detected by automated reconciliation but by manual
    review or external report
  - Break involves a product subject to active recall or safety alert

Step 4: Apply mitigating factors (each may de-escalate severity by one level,
        but never below SEV-3):
  - Break is isolated to a single product unit with no downstream
    dispensation
  - Break was detected proactively (automated reconciliation) before
    any downstream action
  - Compensating evidence is immediately available and confirms no
    impact
  - Break is attributable to a known, documented, and transient system
    issue (e.g., scheduled maintenance window)

Step 5: Final severity = Base severity adjusted by net aggravating/mitigating
factors
        (minimum SEV-4; maximum SEV-1)

Step 6: Log severity assessment with factors documented in break detection
record
```

Severity Override. Institutional governance may override the assessed severity with documented justification. Overrides that reduce severity require dual authorization. Overrides that increase severity require single authorization. All overrides are logged as ILS records.

C.10 Break Lifecycle Summary

Every break, regardless of type or severity, follows this lifecycle:

Lifecycle Stage	ILS Event	Key Actions	SLA (Default)
DETECTED	BRK_DETECTED	Break identified by	Immediate (at

Lifecycle Stage	ILS Event	Key Actions	SLA (Default)
		reconciliation execution; severity assessed; break record generated	reconciliation)
CONTAINED	BRK_CONTAINED	Hold-only containment applied per severity; affected scope identified; investigation assigned	SEV-1: 15 min; SEV-2: 1 hour; SEV-3: 4 hours; SEV-4: next reconciliation cycle
INVESTIGATED	BRK_INVESTIGATED	Root cause analysis; evidence gathering; determination of authoritative state; correction proposal	SEV-1: 48 hours; SEV-2: 5 days; SEV-3: 10 days; SEV-4: 30 days
RESOLVED	BRK_RESOLVED	Correction or compensating evidence applied; post-correction reconciliation confirms alignment	Per investigation findings
CLOSED	BRK_CLOSED	Resolution verified; hold released; break record sealed with complete evidence chain	Within 24 hours of resolution verification
RECERT_CHECK	BRK_RECERT_ASSESSED	Governance assessment of whether break warrants recertification trigger or control improvement	Within 10 business days of closure

Appendix D — Standard Checks Pack (Full List)

D.1 Purpose and Structure

The Standard Checks Pack provides a comprehensive list of examiner and reviewer checks covering all operational domains of the framework. Each check is a discrete, repeatable verification that produces a PASS, FAIL, or NOT_APPLICABLE result with documented evidence references.

Check Structure Convention:

Each check includes:

- **Check ID:** Unique identifier using domain prefix and sequence number.
- **Check Purpose:** The operational control or evidence condition being verified.
- **Evidence Required:** Specific evidence artifacts, logs, or records needed to perform the check.
- **Pass Criteria:** Conditions that must be met for a satisfactory finding.
- **Fail Criteria:** Conditions indicating a deficiency requiring remediation or escalation.
- **Risk Rating:** Low, Moderate, High, or Critical — indicating the impact if a control failure is detected.

Checks are organized by domain. Section 14 presented a representative subset of checks; this appendix provides the complete pack.

D.2 Product Authenticity Checks (AUTH-series)

Check ID	Check Purpose	Pass Criteria	Risk Rating
AUTH-001	Verify CPO exists for all products in dispensation scope	100% of dispensed products have CPO with valid content address	High
AUTH-002	Verify manufacturer identity evidence current per freshness window	All manufacturer credentials verified within applicable freshness window at dispensation time	High
AUTH-003	Verify provenance manifest completeness for sampled products	Sampled provenance manifests show PROV_COMPLETE; no unresolved gaps	Critical
AUTH-004	Verify content-addressed integrity of provenance chain	100% hash chain verifications pass for sampled products	Critical
AUTH-005	Verify authenticity state accurately reflects evidence	AUTH_VERIFIED only where all PAES elements present, current, and consistent	High
AUTH-006	Verify authenticity assessment performed before dispensation	No dispensation events for products in AUTH_NOT_ASSESSED state	High
AUTH-007	Verify PAES manifests are content-addressed and retrievable	Sampled PAES manifests retrievable by content address; integrity verification passes	High
AUTH-008	Verify product identity verification performed at each CUS_RECEIPT	Sampled receipt events include product identity verification result	Moderate
AUTH-009	Verify CPO correction EP Deltas generated for all CPO changes	No CPO modifications without corresponding EP Delta record	Critical
AUTH-010	Verify manufacturer credential	Revocation check logged for manufacturer	High

Check ID	Check Purpose	Pass Criteria	Risk Rating
	revocation check performed at dispensation	credential at each sampled dispensation	

D.3 Provenance and Custody Checks (PROV-series)

Check ID	Check Purpose	Pass Criteria	Risk Rating
PROV-001	Verify custody event chain completeness for sampled products	No undocumented custody gaps in sampled chains	High
PROV-002	Verify handoff confirmation from both sender and receiver	All sampled handoffs have matching sender/receiver confirmation pairs	High
PROV-003	Verify storage condition monitoring active during storage periods	Continuous condition records present for all storage periods in sample	Moderate–High
PROV-004	Verify repackaging events authorized	All CUS_REPACKAGE events linked to authorized repackager credential	High
PROV-005	Verify aggregation hierarchy maintained	All sampled child units traceable to parent aggregation level	Moderate
PROV-006	Verify custody chain integrity at recall scope determination	All affected units identified through aggregation hierarchy; all current custodians notified	Critical
PROV-007	Verify excursion records have corresponding assessments	All CUS_TEMP_EXCURSION events have excursion assessment within SLA	Moderate
PROV-008	Verify custody event attributes complete per minimum requirements	All sampled custody events include required minimum fields (event_id, timestamp, actor, product reference, outcome, integrity_hash, previous_event_hash)	High
PROV-009	Verify custody chain cross-references provenance manifest	Sampled custody events linked to provenance manifest events for the same product	Moderate
PROV-010	Verify no custody events by unauthorized actors	All sampled custody event actor_ids verified against authorized custodian registry	Critical
PROV-011	Verify storage condition baselines defined for product categories	All product categories with condition-sensitive products have documented storage condition baselines	Moderate
PROV-012	Verify destruction events properly documented	All CUS_DESTRUCTION events have authorization record, witness documentation, and disposal evidence	High

D.4 Authorization and Issuer Legitimacy Checks (ISSU-series)

Check ID	Check Purpose	Pass Criteria	Risk Rating
ISSU-001	Verify issuer legitimacy confirmed at dispensation	All sampled dispensation events linked to AES with ISSU_CONFIRMED	Critical
ISSU-002	Verify authorization freshness at	Issuer credential verified within applicable	High

Check ID	Check Purpose	Pass Criteria	Risk Rating
	dispensation time	freshness window at dispensation	
ISSU-003	Verify revocation check performed at dispensation	Revocation check logged for each sampled dispensation; CLEAR result or appropriate handling for non-CLEAR	Critical
ISSU-004	Verify scope-match between authorization and dispensation	Authorization bounds (product, quantity, location, purpose) match dispensation parameters	High
ISSU-005	Verify supersession chain integrity for multi-version authorizations	Ordered chain; no ambiguous current-reference state; dispensation bound to current version	High
ISSU-006	Verify delegation authority where delegated prescribing applies	Delegation instrument current; delegator authority verified; delegation scope matches action	High
ISSU-007	Verify expired authorizations do not support new dispensation	No dispensation events referencing authorization in RX_EXPIRED state at dispensation time	High
ISSU-008	Verify revoked authorizations trigger hold on pending dispensation	All pending dispensation under revoked authorizations held or cancelled	Critical
ISSU-009	Verify AES generated and content-addressed for all authorizations	Sampled authorizations have complete AES with content-addressed integrity	High
ISSU-010	Verify authorization EP Deltas generated for all lifecycle transitions	Each sampled authorization state change (renewal, revocation, supersession, suspension) has corresponding EP Delta	High
ISSU-011	Verify quantity bound tracking across partial dispensation	Accumulated dispensation quantity tracked against authorization quantity bound; threshold breach triggers hold	Moderate
ISSU-012	Verify emergency authorizations subject to post-hoc review	All emergency authorizations reviewed within institutional SLA; review records documented	High

---

D.5 Dispensation Integrity Checks (DISP-series)

Check ID	Check Purpose	Pass Criteria	Risk Rating
DISP-001	Verify all dispensation precondition gates evaluated	All sampled dispensation events have complete gate completion record (G1–G7)	Critical
DISP-002	Verify no gate bypass without documented override	No dispensation where any gate = FAIL without documented override and Exceptional review posture	Critical
DISP-003	Verify dispensation evidence record generated for each release	All sampled CUS_DISPENSATION events have corresponding DEP-H manifest	High
DISP-004	Verify DEP-H cross-references PAES, AES, CES, SES	Sampled DEP-H manifests contain valid content-addressed references to all required upstream evidence sets	High

Check ID	Check Purpose	Pass Criteria	Risk Rating
DISP-005	Verify dispensing entity credential active at dispensation	Dispensing entity credential verified and non-revoked at each sampled dispensation event	High
DISP-006	Verify partial dispensation quantity tracking accurate	For multi-fill prescriptions: accumulated quantity matches sum of individual dispensation records	Moderate
DISP-007	Verify hold-only containment prevents dispensation	No dispensation events for products in HOLD_HELD, HOLD_QUARANTINED, or HOLD_RECALLED state	Critical
DISP-008	Verify dispensation evidence retention per policy	Sampled DEP-H manifests present in storage per retention metadata; no premature destruction	High

D.6 Proof-of-Safety Checks (SAFE-series)

Check ID	Check Purpose	Pass Criteria	Risk Rating
SAFE-001	Verify required safety evidence classes present at dispensation	All required classes per Section 7.2 matrix present for sampled events	High
SAFE-002	Verify safety evidence currency at dispensation time	Evidence classes current relative to source data version at dispensation time	High
SAFE-003	Verify safety alert overrides documented	All overrides linked to DS-05 with documented justification	Critical
SAFE-004	Verify context-bound decision state records for high-impact decisions	High-impact decisions have complete context-bound decision state records with all required fields	High
SAFE-005	Verify decision state replay capability	Sampled decision states can be independently reconstructed from evidence references	High
SAFE-006	Verify superseded safety evidence triggers appropriate action	No dispensation relying on superseded safety evidence without refresh	High
SAFE-007	Verify SES manifests generated and content-addressed	Sampled dispensation events have corresponding SES manifest with valid content address	High
SAFE-008	Verify review posture correctly classified	Sampled decisions classified as Standard, Enhanced, or Exceptional per Section 7.4 criteria; no under-classification	Moderate
SAFE-009	Verify algorithm version tracking in decision state records	Decision state records reference specific algorithm/database versions; version references are valid and retrievable	Moderate
SAFE-010	Verify manual confirmation pathway properly documented	All manual safety confirmations (Section 7.6) have qualified assessor credential, manual assessment record, and Enhanced/Exceptional review posture	High

D.7 Recall, Quarantine, and Correction Checks (RCLL-series)

Check ID	Check Purpose	Pass Criteria	Risk Rating
RCLL-001	Verify recall scope determination complete	All affected units identified; all current custody holders notified	Critical
RCLL-002	Verify recall acknowledgment tracking	All notified custody holders acknowledged within SLA	High
RCLL-003	Verify recalled products quarantined	All identified affected units quarantined, returned, or destroyed with evidence	Critical
RCLL-004	Verify corrections generate EP Deltas	All corrections produce EP Deltas with prior state preserved	Critical
RCLL-005	Verify correction approval chain documented	All material corrections approved by appropriate authority per RACI	High
RCLL-006	Verify downstream propagation of corrections	All downstream events affected by correction identified and addressed	High
RCLL-007	Verify recall closure reconciliation	Recall closure report shows all affected units accounted for; open items = 0 or governance-approved exception	Critical
RCLL-008	Verify no silent overwrites in evidence chain	Periodic hash verification confirms no artifact modification without EP Delta	Critical
RCLL-009	Verify quarantine segregation verification	All CUS_QUARANTINE_ENTRY events have segregation verification evidence	High
RCLL-010	Verify hold release requires documented resolution	All CUS_HOLD_RELEASE events have resolution evidence and approval chain	High
RCLL-011	Verify supersession chains complete and unambiguous	Sampled supersession chains are ordered; single current-reference state determinable; no orphaned versions	High
RCLL-012	Verify historical states preserved non-destructively	Sampled corrected, superseded, and revoked records accessible via original content address	Critical

---

D.8 Reconciliation and Evidence Integrity Checks (RECON-series)

Check ID	Check Purpose	Pass Criteria	Risk Rating
RECON-001	Verify reconciliation executed per cadence matrix	All reconciliation types executed within defined cadence; no overdue cycles	High
RECON-002	Verify break detection records generated for all detected breaks	All breaks have BRK_DETECTED ILS records with severity assessment	High
RECON-003	Verify break containment applied per severity SLA	All SEV-1 and SEV-2 breaks have containment evidence within SLA	Critical
RECON-004	Verify break resolution within SLA	Break resolution times within SLA for each severity band	High
RECON-005	Verify break lifecycle	Sampled breaks show complete lifecycle	High

Check ID	Check Purpose	Pass Criteria	Risk Rating
	completeness	(DETECTED → CONTAINED → INVESTIGATED → RESOLVED → CLOSED)	
RECON-006	Verify open breaks register maintained	Open breaks register current; all unresolved breaks tracked with aging	Moderate
RECON-007	Verify content-addressed storage integrity	Periodic hash verification executed per schedule; no unresolved integrity failures	Critical
RECON-008	Verify evidence chain-of-custody maintained	All evidence access, export, and transfer events documented per Section 9.4	High
RECON-009	Verify evidence retrieval within SLO	Sampled evidence retrieval requests responded within target response times	Moderate
RECON-010	Verify reconciliation reports content-addressed and chained	Sampled reconciliation reports have valid content address; chain linkage to preceding report intact	High
RECON-011	Verify Preservation Bundles generated per trigger criteria	All trigger events (Section 9.7) have corresponding Preservation Bundle	High
RECON-012	Verify legal hold capability functional	Legal hold activation and deactivation tested per governance schedule; retention overrides confirmed	Moderate

---

D.9 Tiered Access Compliance Checks (ACCS-series)

Check ID	Check Purpose	Pass Criteria	Risk Rating
ACCS-001	Verify all Tier 2 access events have dual-control approval	100% of Tier 2 events have documented dual-control approval with independent approvers	Critical
ACCS-002	Verify TTL enforcement for Tier 1 and Tier 2 access	All access grants expired at TTL; no access beyond TTL without documented renewal	High
ACCS-003	Verify post-access review completion for Tier 2 events	All Tier 2 events have completed PARP within 5-business-day SLA	High
ACCS-004	Verify purpose limitation compliance	Evidence accessed consistent with documented purpose code; no scope creep	High
ACCS-005	Verify minimization and redaction in evidence pack exports	Prohibited data elements redacted; minimization applied; redaction logged	High
ACCS-006	Verify Tier 0 outputs contain no individual-identifiable data	Sampled Tier 0 outputs contain aggregate statistics only	High
ACCS-007	Verify Tier 1 uses pseudonymized references	Sampled Tier 1 evidence extracts use pseudonymized actor and subject references	High
ACCS-008	Verify Tier 2 objective triggers documented	All Tier 2 access requests reference predefined objective trigger criteria	Critical
ACCS-009	Verify emergency access procedures followed	Emergency Tier 2 access events have expedited approval and post-hoc	High

Check ID	Check Purpose	Pass Criteria	Risk Rating
		documentation within 24 hours	
ACCS-010	Verify access event logging complete	All access events at all tiers logged as ILS records with required minimum fields	High

D.10 Governance, Recertification, and Accountability Checks (GOVN-series)

Check ID	Check Purpose	Pass Criteria	Risk Rating
GOVN-001	Verify recertification completed per cadence	All recertification cycles completed on schedule; no overdue recertifications	High
GOVN-002	Verify material change triggers documented and responded to	All material change triggers logged; governance response documented within SLA	High
GOVN-003	Verify no-master-key posture maintained	All material governance actions have multi-party approval; no single-party override detected	Critical
GOVN-004	Verify RACI accountability for critical activities	Sampled activities executed per RACI assignments; accountability documented	High
GOVN-005	Verify liability trigger catalog maintained and current	Catalog current; all trigger events logged and responded to per catalog	High
GOVN-006	Verify change control procedures followed for framework changes	All changes to operational standards, reconciliation cadences, or evidence requirements processed through Change Control Board	High
GOVN-007	Verify governance meeting records documented	Steering Committee and Change Control Board meetings documented with decisions and action items	Moderate
GOVN-008	Verify delegation controls maintained	All delegation records current; expired delegations revoked; delegation chains within governance limits	High
GOVN-009	Verify accountability records generated for all corrections and overrides	All corrections, overrides, recalls, and supersession events have accountability records per Section 11.9	High
GOVN-010	Verify incident escalation SLAs met	Sampled incidents escalated within SLA per severity classification	High

D.11 Offboarding Checks (OFFB-series)

Check ID	Check Purpose	Pass Criteria	Risk Rating
OFFB-001	Verify final state snapshot generated and integrity-verified	Snapshot complete; master hash verified; officer attestation present	High
OFFB-002	Verify final reconciliation executed and documented	All reconciliation types executed; results documented; breaks inventoried	High

Check ID	Check Purpose	Pass Criteria	Risk Rating
OFFB-003	Verify open breaks disclosed	All unresolved breaks disclosed; governance approved offboarding with open breaks (if any)	Critical
OFFB-004	Verify legacy transition manifest complete	All evidence types mapped; data loss documented; non-mappable artifacts archived	High
OFFB-005	Verify post-transfer verification completed	Legacy system records match framework evidence at transition point	High
OFFB-006	Verify archival retention applied	All evidence archived per retention requirements; no premature destruction	High
OFFB-007	Verify pre-offboarding requirements met	All active holds resolved or transferred; all open breaks resolved or disclosed; governance approval documented	High
OFFB-008	Verify post-offboarding monitoring initiated	Monitoring schedule established; open break tracking active; archival integrity verification scheduled	Moderate

D.12 Claim / Reimbursement Checks (CLM-series) — Optional

Included only where Section 12 is in scope.

Check ID	Check Purpose	Pass Criteria	Risk Rating
CLM-001	Verify claim evidence gates evaluated at validation	All sampled claims have complete gate results (CG-1 through CG-6)	High
CLM-002	Verify temporal evidence assessment applied	Authorization validity assessed at dispensation time, not claim time, for sampled claims	High
CLM-003	Verify claim-dispensation linkage intact	All sampled claims reference a valid, content-addressed dispensation event	High
CLM-004	Verify no duplicate payouts	No duplicate CLM_PAID events for any single CLM_APPROVED	Critical
CLM-005	Verify post-payment adjustments documented	All CLM_ADJUSTED records have reason, amount delta, and upstream change reference	High
CLM-006	Verify open breaks register maintained for claims	Open breaks register for claims current; all unresolved items tracked with aging	Moderate
CLM-007	Verify claim denial includes appeal pathway	All CLM_DENIED records document reason code and appeal pathway	Moderate
CLM-008	Verify payout settlement confirmation linked to claim	All CLM_PAID events have settlement confirmation with payment reference and amount	High

D.13 Summary Statistics

Domain	Check Series	Check Count	Critical	High	Moderate
Product Authenticity	AUTH-001 to AUTH-010	10	2	7	1
Provenance and Custody	PROV-001 to PROV-012	12	2	7	3
Authorization and Legitimacy	ISSU-001 to ISSU-012	12	2	9	1
Dispensation Integrity	DISP-001 to DISP-008	8	3	4	1
Proof-of-Safety	SAFE-001 to SAFE-010	10	1	7	2
Recall and Correction	RCLL-001 to RCLL-012	12	5	7	0
Reconciliation and Integrity	RECON-001 to RECON-012	12	2	7	3
Tiered Access Compliance	ACCS-001 to ACCS-010	10	2	7	1
Governance and Accountability	GOVN-001 to GOVN-010	10	1	8	1
Offboarding	OFFB-001 to OFFB-008	8	1	6	1
Claims (Optional)	CLM-001 to CLM-008	8	1	5	2
Total		**112**	**22**	**74**	**16**

Appendix E — Reviewer / Examiner Query Pack (Expanded; Conceptual SQL / Pseudocode / Retrieval Logic)

E.1 Purpose and Usage

This appendix provides an expanded set of conceptual queries that reviewers, examiners, auditors, and institutional operators can adapt to their specific retrieval infrastructure. Queries are organized by examiner objective — the operational question the examiner needs answered — rather than by technical domain. Each query includes: the examiner question in plain language, the query family and ID, the evidence sources consulted, the conceptual retrieval logic, and the expected output format.

Section 14.9 provided 12 representative queries across 6 families. This appendix expands to 30 queries across 10 families, covering the full scope of examiner concerns.

Implementation Note. Queries are expressed in SQL-like pseudocode for clarity. Actual implementation will vary by storage technology, indexing approach, and access control layer. The pseudocode assumes relational-style access to ILS records, evidence manifests, and state tables; content-addressed retrieval is represented through hash-based lookups. Tiered access controls (Section 10) apply to all query execution — the query engine must enforce purpose limitation and TTL before returning results.

E.2 Query Family 1: Product Authenticity and Provenance Verification

EQP-001: What is the current authenticity state of a specific product?

Examiner question: "Show me the authenticity evidence for product [CPO reference]."

```
SELECT p.cpo_content_address, p.product_reference_id,
       p.batch_lot_reference, p.authenticity_state,
       p.state_determination_timestamp,
       pm.chain_status AS provenance_status,
       pm.event_count, pm.last_event_hash,
       mfr.legitimacy_state AS manufacturer_state,
       mfr.freshness_status AS manufacturer_freshness
FROM product_authenticity_states p
JOIN provenance_manifests pm
  ON p.cpo_content_address = pm.cpo_reference
LEFT JOIN authorization_evidence_sets mfr
  ON p.manufacturer_credential_ref = mfr.evidence_content_address
WHERE p.cpo_content_address = :target_cpo
ORDER BY p.state_determination_timestamp DESC
```

```
LIMIT 1;
```

Expected output: Single row with authenticity state, provenance chain status, manufacturer credential status, and freshness indicators.

EQP-002: Show all products with unresolved provenance breaks in a date range.

Examiner question: "How many products have provenance issues right now?"

```
SELECT rb.break_id, rb.break_code, rb.severity,
       rb.detected_at, rb.lifecycle_status,
       rb.affected_product_cpo,
       EXTRACT(DAY FROM CURRENT_TIMESTAMP - rb.detected_at) AS age_days,
       rb.assigned_to
FROM reconciliation_breaks rb
WHERE rb.break_code LIKE 'BRK-PROV-%'
  AND rb.lifecycle_status NOT IN ('RESOLVED', 'CLOSED')
  AND rb.detected_at >= :period_start
  AND rb.detected_at <= :period_end
ORDER BY rb.severity, rb.detected_at;
```

Expected output: List of open provenance breaks with aging, severity, and assignment.

EQP-003: Reconstruct the complete provenance chain for a product from manufacture to current custody.

Examiner question: "Walk me through every custody transition for product [reference] from origin."

```
SELECT ce.event_id, ce.event_type, ce.timestamp,
       ce.actor_id, ce.product_cpo_reference,
       ce.previous_event_hash, ce.content_address,
       CASE WHEN ce.previous_event_hash = prev.content_address
            THEN 'CHAIN_INTACT'
            ELSE 'CHAIN_BREAK' END AS integrity_status
FROM custody_events ce
LEFT JOIN custody_events prev
  ON ce.previous_event_hash = prev.content_address
WHERE ce.product_cpo_reference = :target_cpo
ORDER BY ce.timestamp ASC;
```

Expected output: Ordered custody event timeline with integrity verification at each link.

E.3 Query Family 2: Authorization and Prescription Lifecycle

EQP-004: Show the full authorization lifecycle for a prescription.

Examiner question: "What happened to prescription [auth_id] from issuance to current state?"

```
SELECT ed.delta_id, ed.change_type, ed.change_timestamp,
       ed.previous_state, ed.new_state,
       ed.change_authority, ed.change_evidence,
       ed.downstream_impact
FROM ep_deltas ed
WHERE ed.authorization_reference = :target_auth_id
ORDER BY ed.change_timestamp ASC;
```

Expected output: Chronological list of all state transitions with authority and evidence references.

EQP-005: Identify all dispensation events that relied on a subsequently revoked authorization.

Examiner question: "After authorization [auth_id] was revoked, which dispensation events had already occurred under it?"

```
SELECT d.dispensation_event_id, d.timestamp AS dispensation_time,
       d.product_cpo_reference, d.recipient_reference,
       rev.change_timestamp AS revocation_time,
       EXTRACT(DAY FROM rev.change_timestamp - d.timestamp)
         AS days_before_revocation
FROM dispensation_events d
JOIN ep_deltas rev
  ON d.authorization_reference = rev.authorization_reference
  AND rev.new_state = 'RX_REVOKED'
WHERE d.authorization_reference = :target_auth_id
  AND d.timestamp < rev.change_timestamp
ORDER BY d.timestamp;
```

Expected output: List of dispensation events that occurred before the revocation, with gap duration.

EQP-006: Show all active prescriptions from an issuer whose credentials were restricted or revoked.

Examiner question: "Dr. [reference] had credentials restricted — what prescriptions are still active?"

```
SELECT a.authorization_id, a.prescription_validity_state,
       a.product_bound, a.validity_end,
```

```
       aes.legitimacy_state AS current_issuer_state,
       aes.currency_check_timestamp
FROM authorization_states a
JOIN authorization_evidence_sets aes
  ON a.issuer_aes_reference = aes.evidence_content_address
WHERE aes.issuer_reference_id = :target_issuer_ref
  AND aes.legitimacy_state IN ('ISSU_REVOKED', 'ISSU_RESTRICTED')
  AND a.prescription_validity_state NOT IN ('RX_EXPIRED', 'RX_REVOKED',
      'RX_SUPERSEDED')
ORDER BY a.validity_end;
```

Expected output: Active prescriptions from the affected issuer requiring review or re-authorization.

E.4 Query Family 3: Dispensation Gate Compliance

EQP-007: Show gate completion records for all dispensation events in a period.

Examiner question: "Did all dispensations pass their precondition gates?"

```
SELECT d.dispensation_event_id, d.timestamp,
       gc.gate_id, gc.gate_result, gc.failure_reason,
       d.review_posture
FROM dispensation_events d
JOIN gate_completion_records gc
  ON d.dispensation_event_id = gc.dispensation_event_id
WHERE d.timestamp >= :period_start
  AND d.timestamp <= :period_end
  AND gc.gate_result = 'FAIL'
ORDER BY d.timestamp, gc.gate_id;
```

Expected output: All gate failures with associated dispensation events and failure reasons.

EQP-008: Identify dispensation events where gates were bypassed with override.

Examiner question: "Were there any gate overrides, and were they properly documented?"

```
SELECT d.dispensation_event_id, d.timestamp,
       d.review_posture,
       gc.gate_id, gc.gate_result,
       ovr.override_authority, ovr.override_justification,
       ovr.override_documentation_ref
```

```
FROM dispensation_events d
JOIN gate_completion_records gc
  ON d.dispensation_event_id = gc.dispensation_event_id
LEFT JOIN gate_overrides ovr
  ON gc.gate_completion_id = ovr.gate_completion_id
WHERE d.timestamp >= :period_start
  AND gc.gate_result = 'FAIL'
  AND d.dispensation_state = 'DISP_RELEASED'
ORDER BY d.timestamp;
```

Expected output: Gate failures that did not prevent dispensation, with override documentation status.

E.5 Query Family 4: Safety Evidence and Clinical Decision Review

EQP-009: Show all safety alert overrides in a period with override documentation status.

Examiner question: "How often are safety alerts overridden, and is the documentation adequate?"

```
SELECT ds.decision_id, ds.decision_timestamp,
       ds.decision_type, ds.decision_actor,
       ds.algorithm_version,
       ds.override_justification IS NOT NULL AS has_justification,
       ds.review_posture
FROM decision_states ds
WHERE ds.override_flag = TRUE
  AND ds.decision_timestamp >= :period_start
  AND ds.decision_timestamp <= :period_end
ORDER BY ds.decision_timestamp;
```

Expected output: Override inventory with documentation completeness indicator.

EQP-010: For a specific clinical decision, retrieve the complete evidence context that existed at decision time.

Examiner question: "Replay decision [decision_id] — what did the system show and what did the clinician do?"

```
-- Step 1: Retrieve decision state record
SELECT ds.* FROM decision_states ds
WHERE ds.decision_id = :target_decision_id;
```

```
-- Step 2: Retrieve all referenced evidence artifacts
SELECT ea.artifact_id, ea.artifact_type, ea.version,
       ea.content_address, ea.generation_timestamp,
       ea.freshness_status_at_decision_time
FROM evidence_artifacts ea
JOIN decision_evidence_refs der
  ON ea.content_address = der.evidence_content_address
WHERE der.decision_id = :target_decision_id
ORDER BY ea.artifact_type;

-- Step 3: Retrieve algorithm version metadata
SELECT av.algorithm_id, av.version_id, av.release_date,
       av.deprecation_date, av.status
FROM algorithm_versions av
WHERE av.version_id = :decision_algorithm_version;
```

Expected output: Complete decision context: decision record, all evidence artifacts consulted, and algorithm version status.

EQP-011: Identify dispensation events where safety evidence was superseded before next refill.

Examiner question: "Are there active prescriptions where the safety data changed since last dispensation?"

```
SELECT d.dispensation_event_id, d.timestamp AS last_dispensation,
       d.product_cpo_reference, d.authorization_reference,
       ses_update.supersession_timestamp,
       ses_update.change_description,
       next_refill.expected_date AS next_refill_date
FROM dispensation_events d
JOIN safety_evidence_supersessions ses_update
  ON d.product_cpo_reference = ses_update.product_cpo_reference
  AND ses_update.supersession_timestamp > d.timestamp
LEFT JOIN refill_schedule next_refill
  ON d.authorization_reference = next_refill.authorization_reference
  AND next_refill.expected_date > ses_update.supersession_timestamp
WHERE next_refill.dispensation_completed = FALSE
```

```
ORDER BY ses_update.supersession_timestamp;
```

Expected output: Dispensation events with safety evidence changes pending before next refill.

E.6 Query Family 5: Reconciliation and Break Management

EQP-012: Open breaks inventory with aging and SLA compliance.

```
SELECT rb.break_id, rb.break_code, rb.break_name,
       rb.severity, rb.detected_at,
       EXTRACT(DAY FROM CURRENT_TIMESTAMP - rb.detected_at) AS age_days,
       rb.resolution_sla_hours,
       CASE WHEN EXTRACT(HOUR FROM CURRENT_TIMESTAMP - rb.detected_at)
            > rb.resolution_sla_hours THEN 'SLA_BREACHED'
            ELSE 'WITHIN_SLA' END AS sla_status,
       rb.assigned_to, rb.lifecycle_status
FROM reconciliation_breaks rb
WHERE rb.lifecycle_status NOT IN ('RESOLVED', 'CLOSED')
ORDER BY rb.severity, rb.detected_at;
```

EQP-013: Break resolution trend analysis — root causes and resolution times by period.

```
SELECT DATE_TRUNC('month', rb.detected_at) AS period,
       rb.break_code, rb.severity,
       COUNT(*) AS break_count,
       AVG(EXTRACT(HOUR FROM rb.resolved_at - rb.detected_at))
         AS avg_resolution_hours,
       PERCENTILE_CONT(0.95) WITHIN GROUP
         (ORDER BY EXTRACT(HOUR FROM rb.resolved_at - rb.detected_at))
         AS p95_resolution_hours
FROM reconciliation_breaks rb
WHERE rb.lifecycle_status IN ('RESOLVED', 'CLOSED')
  AND rb.detected_at >= :analysis_start
GROUP BY DATE_TRUNC('month', rb.detected_at),
         rb.break_code, rb.severity
ORDER BY period, break_count DESC;
```

EQP-014: Verify reconciliation cadence compliance — were all scheduled reconciliations executed?

```
SELECT rt.reconciliation_type, rt.required_cadence,
       COUNT(re.execution_id) AS executions_in_period,
       rt.expected_executions_in_period,
       CASE WHEN COUNT(re.execution_id) >= rt.expected_executions_in_period
            THEN 'COMPLIANT' ELSE 'NON_COMPLIANT' END AS cadence_status
FROM reconciliation_types rt
LEFT JOIN reconciliation_executions re
  ON rt.reconciliation_type = re.reconciliation_type
  AND re.execution_timestamp >= :period_start
  AND re.execution_timestamp <= :period_end
GROUP BY rt.reconciliation_type, rt.required_cadence,
         rt.expected_executions_in_period;
```

E.7 Query Family 6: Recall Scope and Completeness

EQP-015: For a specific recall, show scope vs. resolution status.

```
SELECT r.recall_id, r.product_cpo_reference,
       r.batch_lot_reference, r.urgency_classification,
       r.total_units_in_scope,
       SUM(CASE WHEN ra.disposition = 'RETURNED' THEN ra.unit_count ELSE 0 END)
         AS units_returned,
       SUM(CASE WHEN ra.disposition = 'DESTROYED' THEN ra.unit_count ELSE 0 END)
         AS units_destroyed,
       SUM(CASE WHEN ra.disposition = 'DISPENSED_PRE_RECALL'
           THEN ra.unit_count ELSE 0 END) AS units_dispensed_pre_recall,
       r.total_units_in_scope -
         SUM(COALESCE(ra.unit_count, 0)) AS units_unaccounted
FROM recalls r
LEFT JOIN recall_acknowledgments ra
  ON r.recall_id = ra.recall_id
WHERE r.recall_id = :target_recall_id
GROUP BY r.recall_id, r.product_cpo_reference,
         r.batch_lot_reference, r.urgency_classification,
         r.total_units_in_scope;
```

EQP-016: Identify custody holders who have not acknowledged a recall within SLA.

```
SELECT r.recall_id, rn.notified_entity_id,
       rn.notification_timestamp,
       rn.acknowledgment_sla_hours,
       EXTRACT(HOUR FROM CURRENT_TIMESTAMP - rn.notification_timestamp)
         AS hours_since_notification,
       CASE WHEN ra.acknowledgment_timestamp IS NULL THEN 'NOT_ACKNOWLEDGED'
            ELSE 'ACKNOWLEDGED' END AS ack_status
FROM recall_notifications rn
JOIN recalls r ON rn.recall_id = r.recall_id
LEFT JOIN recall_acknowledgments ra
  ON rn.recall_id = ra.recall_id
  AND rn.notified_entity_id = ra.acknowledging_entity_id
WHERE r.recall_id = :target_recall_id
  AND ra.acknowledgment_timestamp IS NULL
  AND EXTRACT(HOUR FROM CURRENT_TIMESTAMP - rn.notification_timestamp)
    > rn.acknowledgment_sla_hours
ORDER BY hours_since_notification DESC;
```

E.8 Query Family 7: Tiered Access Compliance

EQP-017: Show all Tier 2 access events with approval and PARP status.

```
SELECT ta.access_event_id, ta.timestamp, ta.actor_id,
       ta.purpose_code, ta.trigger_condition,
       ta.approval_officer_1, ta.approval_officer_2,
       ta.ttl_expiry,
       parp.review_timestamp AS parp_completed,
       CASE WHEN parp.review_timestamp IS NULL THEN 'PARP_MISSING'
            WHEN parp.review_timestamp >
              ta.ttl_expiry + INTERVAL '5 days' THEN 'PARP_OVERDUE'
            ELSE 'PARP_COMPLETE' END AS parp_status
FROM tier2_access_events ta
LEFT JOIN post_access_review_packs parp
  ON ta.access_event_id = parp.access_event_reference
WHERE ta.timestamp >= :period_start
ORDER BY ta.timestamp;
```

EQP-018: Access volume and purpose distribution across all tiers.

```
SELECT ta.tier_level, ta.purpose_code,
       COUNT(*) AS access_count,
       COUNT(DISTINCT ta.actor_id) AS unique_reviewers,
       AVG(EXTRACT(HOUR FROM ta.ttl_expiry - ta.timestamp))
         AS avg_ttl_hours
FROM all_access_events ta
WHERE ta.timestamp >= :period_start
GROUP BY ta.tier_level, ta.purpose_code
ORDER BY ta.tier_level, access_count DESC;
```

E.9 Query Family 8: Governance and Accountability

EQP-019: Show all liability trigger events in a period with response status.

```
SELECT lt.trigger_id, lt.trigger_code, lt.condition_description,
       lt.severity, lt.detected_at,
       lt.immediate_action_taken, lt.escalation_record_ref,
       lt.resolution_status,
       pb.preservation_bundle_id
FROM liability_trigger_events lt
LEFT JOIN preservation_bundles pb
  ON lt.trigger_id = pb.trigger_reference
WHERE lt.detected_at >= :period_start
ORDER BY lt.severity, lt.detected_at;
```

EQP-020: Verify no single-party overrides of governance controls.

```
SELECT ar.event_id, ar.event_type, ar.timestamp,
       ar.actor_id, ar.authority_reference,
       ar.approval_chain,
       CASE WHEN JSON_ARRAY_LENGTH(ar.approval_chain) < 2
            THEN 'SINGLE_PARTY_VIOLATION'
            ELSE 'MULTI_PARTY_COMPLIANT' END AS approval_status
FROM accountability_records ar
WHERE ar.event_type IN ('CORRECTION', 'OVERRIDE', 'HOLD_RELEASE',
      'RECALL_CLOSURE', 'TIER2_GRANT', 'GOVERNANCE_ACTION')
  AND ar.timestamp >= :period_start
```

```
  AND JSON_ARRAY_LENGTH(ar.approval_chain) < 2
ORDER BY ar.timestamp;
```

Expected output: Any governance actions executed with fewer than 2 approvers — should be empty if no-master-key posture maintained.

E.10 Query Family 9: Offboarding Verification

EQP-021: Verify offboarding completeness — final snapshot, reconciliation, and open breaks.

```
SELECT ob.offboarding_id, ob.offboarding_trigger,
       ob.final_snapshot_hash, ob.final_snapshot_verified,
       ob.final_reconciliation_executed,
       ob.open_breaks_count, ob.open_breaks_governance_approved,
       ob.legacy_transition_manifest_hash,
       ob.post_transfer_verification_result
FROM offboarding_records ob
WHERE ob.offboarding_id = :target_offboarding_id;
```

EQP-022: Compare evidence counts between framework and legacy system post-transfer.

```
SELECT ltm.evidence_type,
       ltm.framework_artifact_count,
       ltm.legacy_record_count,
       ltm.framework_artifact_count - ltm.legacy_record_count AS delta,
       ltm.data_loss_items, ltm.data_loss_mitigation
FROM legacy_transition_manifests ltm
WHERE ltm.offboarding_id = :target_offboarding_id
ORDER BY ABS(ltm.framework_artifact_count - ltm.legacy_record_count) DESC;
```

E.11 Query Family 10: Claim and Reimbursement (Optional)

EQP-023: Show claims with evidence gate failures and their resolution.

```
SELECT c.claim_id, c.submission_timestamp, c.claim_status,
       cg.gate_id, cg.gate_result, cg.failure_reason,
       cr.resolution_action, cr.resolution_timestamp
FROM claims c
JOIN claim_evidence_gates cg ON c.claim_id = cg.claim_id
LEFT JOIN claim_gate_resolutions cr ON cg.gate_id = cr.gate_id
  AND c.claim_id = cr.claim_id
```

```
WHERE cg.gate_result = 'FAIL'
  AND c.submission_timestamp >= :period_start
ORDER BY c.submission_timestamp;
```

EQP-024: Post-payment adjustment and reversal inventory with upstream triggers.

```
SELECT adj.claim_id, adj.adjustment_type,
       adj.adjustment_amount, adj.adjustment_reason,
       adj.upstream_change_type, adj.upstream_change_reference,
       adj.adjustment_timestamp, adj.recovery_status
FROM claim_adjustments adj
WHERE adj.adjustment_timestamp >= :period_start
ORDER BY adj.adjustment_timestamp;
```

E.12 Query Summary Table

Query ID	Examiner Question (Summary)	Family	Tier Level
EQP-001	Current authenticity state of a product	Authenticity	Tier 1
EQP-002	Open provenance breaks inventory	Authenticity	Tier 0 / Tier 1
EQP-003	Complete provenance chain replay	Authenticity	Tier 1
EQP-004	Authorization lifecycle timeline	Authorization	Tier 1
EQP-005	Dispensation under subsequently revoked authorization	Authorization	Tier 1
EQP-006	Active prescriptions from restricted issuer	Authorization	Tier 1
EQP-007	Gate failures for dispensation events	Dispensation	Tier 1
EQP-008	Gate overrides with documentation status	Dispensation	Tier 1
EQP-009	Safety alert override inventory	Safety	Tier 1
EQP-010	Decision context replay	Safety	Tier 1
EQP-011	Superseded safety evidence before refill	Safety	Tier 1
EQP-012	Open breaks with aging and SLA	Reconciliation	Tier 0 / Tier 1
EQP-013	Break trend analysis	Reconciliation	Tier 0
EQP-014	Reconciliation cadence compliance	Reconciliation	Tier 0
EQP-015	Recall scope vs. resolution	Recall	Tier 1
EQP-016	Overdue recall acknowledgments	Recall	Tier 1
EQP-017	Tier 2 access with PARP status	Access	Tier 0 / Tier 1
EQP-018	Access volume by tier and purpose	Access	Tier 0
EQP-019	Liability trigger events with response	Governance	Tier 1
EQP-020	Single-party override detection	Governance	Tier 1
EQP-021	Offboarding completeness verification	Offboarding	Tier 1
EQP-022	Post-transfer evidence count comparison	Offboarding	Tier 1
EQP-023	Claim gate failures and resolution	Claims	Tier 1
EQP-024	Post-payment adjustments inventory	Claims	Tier 1

Appendix F — Preservation Bundle and Hold-Set Templates

F.1 Preservation Bundle Manifest Template

A Preservation Bundle (PB) is a sealed, content-addressed evidence collection assembled for incidents, disputes, recalls, investigations, or legal holds. This template defines the standard structure.

PB Manifest Template:

```
preservation_bundle:
  bundle_id: PB-[DOMAIN]-[YYYY]-[SEQUENCE]
    # Example: PB-PROV-2026-0045, PB-RECALL-2026-0012
  trigger:
    trigger_type: RECONCILIATION_BREAK | RECALL | SAFETY_INCIDENT |
                  TIER2_ACCESS | DISPUTE | LEGAL_HOLD | INTEGRITY_FAILURE |
                  LIABILITY_TRIGGER | OFFBOARDING
    trigger_reference: [content_address or event_id of triggering event]
    trigger_timestamp: [UTC]
    trigger_severity: SEV-1 | SEV-2 | SEV-3
    trigger_description: [plain-language description]
  scope:
    affected_products: [list of CPO references]
    affected_authorizations: [list of authorization IDs]
    affected_custody_chains: [list of custody chain references]
    affected_dispensation_events: [list of dispensation event IDs]
    affected_claims: [list of claim IDs, if Section 12 in scope]
    time_window: {start: [UTC], end: [UTC]}
  contents:
    detection_artifacts:
      - artifact_id: [content_address]
        artifact_type: [break_detection | recall_notification |
                        incident_report | access_request | ...]
        description: [brief description]
    containment_artifacts:
      - artifact_id: [content_address]
        artifact_type: [hold_entry | quarantine_entry |
                        segregation_verification | ...]
```

```
      description: [brief description]
  investigation_artifacts:
    - artifact_id: [content_address]
      artifact_type: [investigation_log | root_cause_analysis |
                      evidence_snapshot | ...]
      description: [brief description]
  resolution_artifacts:
    - artifact_id: [content_address]
      artifact_type: [correction_ep_delta | determination_record |
                      release_authorization | ...]
      description: [brief description]
  post_review_artifacts:
    - artifact_id: [content_address]
      artifact_type: [post_access_review | lessons_learned |
                      recert_assessment | ...]
      description: [brief description]
  upstream_evidence_sets:
    paes_references: [list of content addresses]
    aes_references: [list of content addresses]
    ces_references: [list of content addresses]
    ses_references: [list of content addresses]
    dep_h_references: [list of content addresses]
    clm_ep_references: [list of content addresses, if applicable]
integrity:
  manifest_hash: [SHA-256 of complete manifest]
  individual_artifact_hashes:
    - artifact_id: [content_address]
      verified: true | false
  chain_verification: PASS | FAIL
lifecycle:
  created_at: [UTC]
  created_by: [role-based identifier]
  sealed_at: [UTC]  # null if still open
  sealed_by: [role-based identifier]
  legal_hold_status: true | false
```

```
    legal_hold_reference: [hold instruction reference, if applicable]
  retention:
    retention_class: PRESERVATION
    retention_period: INDEFINITE | [specific period]
    destruction_prohibited_until: [date or INDEFINITE]
  chain_of_custody:
    - action: creation
      timestamp: [UTC]
      actor: [identifier]
      justification: [trigger reference]
    - action: artifact_added
      timestamp: [UTC]
      actor: [identifier]
      artifact_count: [integer]
    - action: sealed
      timestamp: [UTC]
      actor: [identifier]
      attestation: [officer attestation reference]
  bundle_content_address: [self-referential hash of complete manifest]
```

F.2 Preservation Bundle Templates by Trigger Type

F.2.1 Reconciliation Break Preservation Bundle

Manifest Section	Required Contents for Break PB
detection_artifacts	Break detection ILS record; reconciliation execution report that identified the break; severity assessment record
containment_artifacts	Hold-only containment record (CUS_HOLD_ENTRY or equivalent); containment verification evidence
investigation_artifacts	Root cause analysis report; evidence snapshots (before/after states); transaction logs for affected period; differential analysis
resolution_artifacts	Correction EP Delta (if correction applied); resolution approval record; post-correction reconciliation report confirming alignment
post_review_artifacts	Break closure record; lessons learned document (if material break); recert trigger assessment
upstream_evidence_sets	PAES, AES, CES, SES for affected product and authorization scope

F.2.2 Recall Preservation Bundle

Manifest Section	Required Contents for Recall PB
detection_artifacts	Recall notification record; scope determination with aggregation hierarchy traversal; urgency classification

Manifest Section	Required Contents for Recall PB
containment_artifacts	Quarantine entry records for all affected units; inventory assessment records from custody holders
investigation_artifacts	Recall acknowledgment tracking records; recall scope correction EP Deltas (if scope changed); patient notification records (pseudonymized)
resolution_artifacts	Return/destruction evidence for all resolved units; recall closure report with scope vs. resolution reconciliation
post_review_artifacts	Post-recall assessment; lessons learned; recert trigger assessment
upstream_evidence_sets	PAES for recalled product; CES for all custody holders of recalled batch/lot

F.2.3 Safety Incident Preservation Bundle

Manifest Section	Required Contents for Safety Incident PB
detection_artifacts	Incident detection record; adverse event report (if applicable); safety alert records
containment_artifacts	Product hold or quarantine records; dispensation hold records; patient notification records (pseudonymized)
investigation_artifacts	Product PAES; authorization AES; custody CES; safety SES; context-bound decision state records; dispensation DEP-H
resolution_artifacts	Investigation determination; corrective action records; product disposition (cleared, quarantined, recalled)
post_review_artifacts	Safety review report; institutional corrective action plan; regulatory notification records (if applicable)
upstream_evidence_sets	Complete evidence chain from product manufacture through dispensation

F.2.4 Tier 2 Access Preservation Bundle

Manifest Section	Required Contents for Tier 2 PB
detection_artifacts	Tier 2 access request with objective trigger documentation; dual-control approval records
containment_artifacts	Access scope definition; TTL assignment; purpose code documentation
investigation_artifacts	Evidence accessed inventory (list of artifact content addresses accessed); access event logs; findings document
resolution_artifacts	Investigation determination; referral or closure record
post_review_artifacts	Post-Access Review Pack (PARP); scope compliance verification; participant notification record or deferral justification
upstream_evidence_sets	All evidence sets accessed during Tier 2 investigation

---

F.3 Hold-Set Template

A hold-set is a structured record documenting the scope, authority, and conditions of a hold-only containment action. Hold-sets are maintained as active records during the hold period and become part of the Preservation Bundle at hold release or investigation closure.

Hold-Set Record Template:

```
hold_set:
  hold_id: HOLD-[DOMAIN]-[YYYY]-[SEQUENCE]
```

```
  # Example: HOLD-CUST-2026-0088
hold_type: EVIDENCE_HOLD | REGULATORY_HOLD | RECALL_HOLD |
           DISPUTE_HOLD | SAFETY_HOLD | INVESTIGATION_HOLD
authority:
  hold_authority_role: [role identifier per RACI]
  hold_authority_entity: [pseudonymized entity identifier]
  approval_chain:
    - approver: [identifier]
      approval_timestamp: [UTC]
      approval_method: [digital signature | documented approval]
    - approver: [identifier]  # second approver if dual-control required
      approval_timestamp: [UTC]
scope:
  affected_products:
    - cpo_reference: [content_address]
      unit_count: [integer]
      aggregation_level: UNIT | PACKAGE | CASE | BATCH
  affected_authorizations: [list of authorization IDs]
  affected_dispensation_events: [list of event IDs — pending only]
  affected_claims: [list of claim IDs, if applicable]
conditions:
  hold_reason_code: [BRK code | RECALL reference | SAFETY reference |
                     REGULATORY reference | DISPUTE reference]
  hold_reason_description: [plain-language description]
  hold_start_timestamp: [UTC]
  expected_duration: [hours or "UNTIL_RESOLVED"]
  maximum_duration_before_escalation: [hours]
  escalation_target: [governance body or regulatory authority]
restrictions:
  dispensation_blocked: true
  transfer_blocked: true | false  # transfer may be permitted for
                                  # quarantine movement
  claim_progression_blocked: true | false
  custody_state_changes_blocked: true  # except quarantine and
                                       # investigation events
```

```
monitoring:
  monitoring_cadence: [daily | weekly | per governance determination]
  monitoring_responsible: [role identifier]
  last_review_timestamp: [UTC]
  next_review_due: [UTC]
resolution:  # populated at hold release
  resolution_type: RELEASED | ESCALATED | TRANSFERRED |
                   CONVERTED_TO_RECALL
  resolution_timestamp: [UTC]
  resolution_evidence: [content_address of resolution documentation]
  resolution_authority:
    - approver: [identifier]
      approval_timestamp: [UTC]
  post_release_verification: [content_address of verification record]
evidence_linkage:
  triggering_break: [break_id, if applicable]
  triggering_recall: [recall_id, if applicable]
  preservation_bundle: [PB reference, if PB triggered]
hold_set_content_address: [self-referential hash]
```

F.4 Hold-Set Lifecycle Events

Each hold-set generates ILS records at each lifecycle transition:

Lifecycle Event	ILS Event Code	Required Fields	SLA
Hold placed	CUS_HOLD_ENTRY	hold_id, authority, scope, reason, restrictions	SEV-1: immediate; SEV-2: <1 hour; SEV-3: <4 hours
Hold reviewed (periodic)	HOLD_REVIEWED	hold_id, review_timestamp, reviewer, continued_justification	Per monitoring cadence
Hold escalated	HOLD_ESCALATED	hold_id, escalation_reason, escalation_target, escalation_timestamp	When maximum duration exceeded without resolution
Hold released	CUS_HOLD_RELEASE	hold_id, resolution_type, resolution_evidence, approval_chain, verification_record	Within 4 hours of resolution determination
Hold converted	HOLD_CONVERTED	hold_id, conversion_target (recall_id), conversion_authority	Per governance determination

Lifecycle Event	ILS Event Code	Required Fields	SLA
(e.g., to recall)			

F.5 Legal Hold Activation Template

Legal holds require specific additional controls beyond operational holds.

Legal Hold Activation Record:

```
legal_hold:
  hold_reference: LH-[YYYY]-[SEQUENCE]
  activation:
    activation_authority: [legal counsel or regulatory authority identifier]
    activation_document: [content_address of hold instruction]
    activation_timestamp: [UTC]
    scope_description: [plain-language description of evidence scope]
  scope:
    evidence_types_in_scope: [list: PAES, AES, CES, SES, DEP-H, CLM-EP,
                               ILS, PB, accountability_records]
    product_scope: [CPO references or "ALL_PRODUCTS_IN_RANGE"]
    time_scope: {start: [UTC], end: [UTC] or "ONGOING"}
    entity_scope: [affected institutional participants]
  retention_override:
    standard_retention_suspended: true
    destruction_prohibited: true
    override_effective_until: [date or "UNTIL_RELEASED"]
  monitoring:
    hold_custodian: [designated responsible party]
    compliance_verification_cadence: MONTHLY
    last_verification: [UTC]
  release:  # populated at hold release
    release_authority: [same authority level as activation]
    release_document: [content_address of release instruction]
    release_timestamp: [UTC]
    post_release_retention: [standard retention resumes | specific period]
  legal_hold_content_address: [self-referential hash]
```

Appendix G — RACI Matrices + Accountability Inserts

G.1 Purpose and Conventions

RACI matrices define accountability for critical operational activities across participant roles. Conventions follow Baseline C's RACI structure:

- **R (Responsible):** Performs the work; produces the evidence artifact.
- **A (Accountable):** Ultimately answerable; approves the output; one A per activity.
- **C (Consulted):** Provides input or expertise before the activity is performed.
- **I (Informed):** Notified of the outcome after the activity is completed.

Role Abbreviations Used:

Abbreviation	Role
MFR	Manufacturer or marketing authorization holder
DIST	Distributor / logistics provider
PHRM	Pharmacy / dispensing entity
HOSP	Hospital / institutional healthcare facility
PRSC	Prescriber / authorizing clinician
CRED	Credentialing body / authority
GOV	Framework governance body (Steering Committee / Change Control Board)
SURV	Surveillance / monitoring function
EXAM	Examiner support / regulatory liaison
BENE	Benefit administrator / payer (optional, Section 12 scope)

G.2 RACI Matrix — Product Authenticity and Provenance

Activity	MFR	DIST	PHRM/ HOSP	GOV	SURV	EXAM
Generate Canonical Product Object (CPO)	R/A	I	I	I	I	I
Maintain provenance manifest	R	R	R (own segment)	I	I	C
Verify product identity at receipt (CUS_RECEIPT)	C	R	R	I	I	I
Generate and store PAES	R (origin)	R (additions)	R (additions)	I	C	I
Detect provenance break (BRK-PROV)	C	R	R	I	R/A	C
Contain provenance break (hold-only)	C	R/A	R/A	C	I	I
Investigate provenance break	R (if origin)	R	R	C	R/A	C
Resolve provenance break (correction/determination)	R	R	R	A	C	I

Activity	MFR	DIST	PHRM/ HOSP	GOV	SURV	EXAM
Initiate product recall	R/A	I	I	I	I	I
Track recall scope and acknowledgments	R	R	R	C	R/A	C
Close recall with scope reconciliation	R/A	R	R	A	C	I

G.3 RACI Matrix — Authorization, Prescription, and Issuer Legitimacy

Activity	PRSC	PHRM/ HOSP	CRED	GOV	SURV	EXAM
Issue prescription / authorization	R/A	I	I	I	I	I
Verify issuer legitimacy at dispensation	I	R/A	C	I	I	I
Generate and store AES	I	R	C	I	I	I
Perform revocation check at dispensation	I	R/A	C	I	I	I
Perform scope-match verification	I	R/A	I	I	I	I
Detect authorization break (BRK-AUTH)	I	R	C	I	R/A	C
Contain authorization break (hold pending dispensation)	I	R/A	I	C	I	I
Revoke authorization (prescriber-initiated)	R/A	I	I	I	I	I
Revoke authorization (governance-initiated)	C	I	C	R/A	I	I
Manage supersession chain	R	R	I	I	I	I
Verify delegation authority	I	R/A	C	I	I	I
Emergency authorization review (post-hoc)	R	R	C	A	C	I

G.4 RACI Matrix — Chain-of-Custody and Dispensation

Activity	MFR	DIST	PHRM/HOSP	GOV	SURV	EXAM
Log custody events (CUS_ taxonomy)	R	R	R	I	I	I
Maintain storage condition monitoring	R	R	R	I	I	I
Assess storage excursions	R	R	R	I	C	I
Generate and store CES	R (origin)	R	R	I	C	I
Execute dispensation precondition gates	I	I	R/A	I	I	I
Document dispensation (DEP-H)	I	I	R/A	I	I	I
Detect custody break (BRK-CUST)	I	R	R	I	R/A	C
Contain custody break (hold-only)	I	R/A	R/A	C	I	I
Investigate custody break	C	R	R	C	R/A	C
Execute product quarantine	I	R	R	I	I	I
Process product returns	I	R	R	I	I	I
Document product destruction	I	R/A	R/A	I	I	I

G.5 RACI Matrix — Proof-of-Safety and Clinical Decision Evidence

Activity	PRSC	PHRM/ HOSP	MFR	GOV	SURV	EXAM
Generate safety evidence (PS-01 through PS-05)	I	R	R (PS-01, PS-02)	I	I	I
Generate decision-level evidence (DS-01 through DS-05)	R (DS-05)	R (DS-01–DS-04)	I	I	I	I
Generate and store SES	I	R/A	C	I	I	I
Record context-bound decision states	R	R	I	I	I	I
Document safety alert overrides (DS-05)	R/A	C	I	I	I	I
Detect safety evidence break (BRK-SAFE)	I	R	C	I	R/A	C
Contain safety break (dispensation hold)	I	R/A	I	C	I	I
Refresh superseded safety evidence	I	R	R (provide updates)	I	I	I
Execute manual confirmation pathway	I	R/A	I	I	I	I
Post-decision review (Exceptional posture)	C	R	I	A	C	I

G.6 RACI Matrix — Reconciliation and Evidence Integrity

Activity	MFR	DIST	PHRM/ HOSP	GOV	SURV	EXAM
Execute scheduled reconciliation	I	R	R	I	R/A	I
Detect reconciliation breaks	I	C	C	I	R/A	C
Classify break severity	I	C	C	C	R/A	I
Apply containment per severity	I	R	R	C	A	I
Investigate breaks (root cause)	R (if origin)	R	R	C	R/A	C
Approve break resolution	I	C	C	A	C	I
Execute post-resolution reconciliation	I	C	C	I	R/A	I
Close break record	I	I	I	I	R/A	I
Generate Preservation Bundle	I	R	R	I	R/A	I
Maintain open breaks register	I	I	I	I	R/A	C
Verify content-addressed storage integrity	I	I	I	I	R/A	C
Respond to evidence retrieval requests	R	R	R	I	C	R/A

G.7 RACI Matrix — Tiered Access and Governance

Activity	GOV	SURV	EXAM	PHRM/HOSP	CRED
Approve Tier 1 access requests	R/A	C	R (request)	I	I
Approve Tier 2 access requests (dual-control)	R/A	C	R (request)	I	I
Execute post-access review (PARP)	R	C	I	I	I
Monitor Tier 2 access frequency	I	R/A	I	I	I
Maintain purpose code registry	R/A	C	C	I	I
Execute recertification cycles	R/A	C	I	R (self-assessment)	C
Process material change triggers	R/A	R (detection)	I	R (notification)	C
Maintain liability trigger catalog	R/A	C	C	I	I
Operate Change Control Board	R/A	C	I	C	I
Document governance decisions	R/A	I	I	I	I
Enforce no-master-key posture	R/A	C	C	C	I

G.8 RACI Matrix — Claim and Reimbursement (Optional)

Included only where Section 12 is in scope.

Activity	PHRM/HOSP	BENE	GOV	SURV	EXAM
Submit claim (CLM_SUBMITTED)	R/A	I	I	I	I
Evaluate claim evidence gates (CG-1–CG-6)	I	R/A	I	I	I
Adjudicate claim	I	R/A	I	I	I
Execute payout	I	R/A	I	I	I
Detect claim break (BRK-CLAIM)	C	R	I	R/A	C
Contain claim break (hold)	C	R/A	C	I	I
Execute post-payment adjustment / reversal	C	R/A	C	I	I
Maintain open breaks register (claims)	I	R	I	R/A	C
Respond to claim-related examiner queries	R	R	I	C	R/A

G.9 Accountability Inserts

Accountability inserts are standardized documentation blocks appended to governance actions, corrections, overrides, and escalation decisions. Each insert records the essential accountability information in a consistent format.

Accountability Insert Template:

Field	Content
Insert ID	AI-[YYYY]-[SEQUENCE]
Action type	CORRECTION / OVERRIDE / HOLD_RELEASE / RECALL_CLOSURE / TIER2_GRANT / DELEGATION / MATERIAL_CHANGE /

Field	Content
	GOVERNANCE_DECISION
Action timestamp	[UTC]
Acting entity	[role-based or pseudonymized identifier]
Authority basis	[governance approval reference / delegation instrument / regulatory authority / institutional policy]
Justification	[plain-language justification with evidence references]
Approval chain	[list of approvers with timestamps — minimum 2 for material actions]
Affected scope	[products, authorizations, dispensation events, claims affected]
Downstream impact assessment	[assessment of actions that relied on pre-change state; required re-verification or adjustment actions]
Evidence references	[content addresses of supporting evidence artifacts]
Preservation bundle reference	[PB reference if action triggered preservation]
Insert content address	[self-referential hash for tamper detection]

Insert Application Rules:

- Every accountability record (Section 11.9) must include an accountability insert.
- Inserts are stored as ILS records with content-addressed integrity.
- Inserts are retrievable by the examiner query pack (EQP-019, EQP-020) for governance compliance review.
- Missing inserts for material governance actions constitute a governance violation (GOVN-009 check failure).
- Inserts are retained for the longest of: the affected evidence retention period, the institutional governance retention requirement, and any applicable legal hold.

Appendix H — Content-Addressed Manifest, Diff, and Retrieval Templates

H.1 Purpose

This appendix provides paste-ready templates for the three core content-addressed artifact types used throughout the framework: manifests (evidence inventories), diffs (state change records), and retrieval requests (examiner-initiated evidence production). All templates follow Baseline C's content-addressed storage conventions and are implementation-agnostic.

H.2 Content-Addressed Manifest Template (Generic)

Every evidence collection in the framework — PAES, AES, CES, SES, DEP-H, CLM-EP, Preservation Bundles, offboarding proof bundles — is indexed by a manifest. This generic template defines the common structure; domain-specific manifests (Appendix B) extend it with additional fields.

```
manifest:
  # --- IDENTITY ---
  manifest_id: [content_address — computed after all fields populated]
  manifest_type: PAES | AES | CES | SES | DEP-H | CLM-EP | PB |
                 OFFBOARDING | RECONCILIATION | PROVENANCE
  manifest_version: [integer — incremented on each update]
  supersedes: [content_address of prior version, null if genesis]

  # --- SUBJECT ---
  subject:
    subject_type: PRODUCT | AUTHORIZATION | CUSTODY_CHAIN |
                  DISPENSATION | DECISION | CLAIM | SCOPE_BUNDLE
    subject_reference: [content_address or identifier of subject]
    subject_description: [human-readable; e.g., "Product X, LOT-2026-0955"]

  # --- TIME RANGE ---
  period:
    period_start: [UTC]
    period_end: [UTC]
    snapshot_timestamp: [UTC — when this manifest was generated]

  # --- ARTIFACT INVENTORY ---
```

```
artifacts:
  - artifact_id: [content_address]
    artifact_type: [ILS | EP_DELTA | CONDITION_LOG | CREDENTIAL_REF |
                    GATE_RECORD | DECISION_STATE | RECON_REPORT |
                    EXCURSION_RECORD | HOLD_SET | RECALL_RECORD | ...]
    artifact_timestamp: [UTC — when the artifact was created]
    artifact_description: [brief human-readable description]
    integrity_verified: true | false
    integrity_verification_timestamp: [UTC]
  - ... [repeated for each artifact in the manifest]

# --- COMPLETENESS ---
completeness:
  required_artifact_types: [list of artifact types required for this
                            manifest type per framework rules]
  present_artifact_types: [list of types actually present]
  missing_artifact_types: [list of types missing, with reason codes]
  completeness_percentage: [0–100]
  gaps_documented: true | false

# --- CROSS-REFERENCES ---
linked_manifests:
  - manifest_type: [type of linked manifest]
    manifest_id: [content_address]
    relationship: DEPENDS_ON | REFERENCED_BY | SUPERSEDES | PART_OF
  - ...

# --- INTEGRITY ---
integrity:
  hash_algorithm: SHA-256
  artifact_hashes_verified: [count verified / count total]
  chain_verification_result: PASS | FAIL | NOT_APPLICABLE
  manifest_content_address: [self-referential hash — computed last]

# --- LIFECYCLE ---
```

```
  lifecycle:
    created_at: [UTC]
    created_by: [role-based identifier]
    last_updated_at: [UTC]
    last_updated_by: [role-based identifier]
    sealed: true | false
    sealed_at: [UTC, if sealed]

  # --- RETENTION ---
  retention:
    retention_class: [per Section 9.7 / Baseline C retention taxonomy]
    retention_period: [years or INDEFINITE]
    legal_hold_status: false | true
    destruction_eligible_date: [date, if not under legal hold]
```

H.3 EP Delta (State Change Diff) Template

EP Deltas document state transitions for any evidence artifact, authorization, product state, or reconciliation record. They are the primary mechanism for non-destructive correction and supersession tracking.

```
ep_delta:
  # --- IDENTITY ---
  delta_id: [content_address — computed after all fields populated]
  delta_sequence: [integer — position in the delta chain for this subject]

  # --- SUBJECT ---
  subject_reference: [content_address of the artifact or state being changed]
  subject_type: PRODUCT_STATE | AUTHORIZATION_STATE | CUSTODY_STATE |
                SAFETY_STATE | HOLD_STATE | CLAIM_STATE | EVIDENCE_ARTIFACT |
                CPO | PROVENANCE_MANIFEST | SUPERSESSION_CHAIN

  # --- CHANGE DESCRIPTION ---
  change:
    change_type: CORRECTION | SUPERSESSION | REVOCATION | SUSPENSION |
                 REINSTATEMENT | SCOPE_MODIFICATION | RENEWAL | EXPIRY |
                 RECLASSIFICATION | RECALL_SCOPE_CHANGE | HOLD_ENTRY |
```

```
                HOLD_RELEASE | FRESHNESS_REFRESH
    previous_state: [state value or content_address of prior version]
    new_state: [state value or content_address of new version]
    change_timestamp: [UTC]
    change_description: [human-readable explanation]

  # --- AUTHORITY ---
  authority:
    change_authority: [role-based identifier of entity causing the change]
    authority_basis: [governance_approval | credential_event | regulatory_action
|
                      automated_detection | institutional_policy |
prescriber_action]
    approval_chain:
      - approver_id: [identifier]
        approval_timestamp: [UTC]
      - approver_id: [identifier]  # second approver if required
        approval_timestamp: [UTC]

  # --- EVIDENCE ---
  change_evidence:
    supporting_evidence: [content_address of evidence justifying the change]
    investigation_reference: [break_id or incident_id, if applicable]

  # --- DOWNSTREAM IMPACT ---
  downstream_impact:
    affected_dispensation_events: [count or list of event IDs]
    affected_claims: [count or list of claim IDs]
    affected_custody_chains: [count or list of chain references]
    hold_actions_triggered: [count or list of hold IDs]
    notification_records: [content_addresses of notifications sent]
    propagation_status: COMPLETE | IN_PROGRESS | NOT_REQUIRED

  # --- CHAIN LINKAGE ---
  chain:
    previous_delta_hash: [content_address of preceding EP Delta for this
```

```
                        subject, null if first delta]
  delta_content_address: [self-referential hash — computed last]
```

Diff Chaining. EP Deltas for the same subject form a content-addressed chain. Each delta contains the hash of the preceding delta, enabling a reviewer to traverse the complete change history from the current state back to the original. Chain integrity is verifiable through hash validation at each link.

Diff Optimization. Only changed fields are recorded in the change section. Unchanged fields are omitted from the diff to reduce storage overhead. The previous_state and new_state fields contain complete state values (not partial diffs), enabling independent interpretation of each delta without requiring access to the full artifact.

H.4 Retrieval Request Template

Retrieval requests are the formal mechanism by which reviewers, examiners, and institutional operators request evidence from the framework's content-addressed storage. Retrieval requests enforce tiered access controls, purpose limitation, and TTL.

```
retrieval_request:
  # --- REQUEST IDENTITY ---
  request_id: [unique identifier]
  request_timestamp: [UTC]

  # --- REQUESTER ---
  requester:
    requester_id: [role-based or pseudonymized identifier]
    requester_role: [EXAMINER | AUDITOR | INSTITUTIONAL_REVIEWER |
                     GOVERNANCE_BODY | INCIDENT_INVESTIGATOR |
                     DISPUTE_AUTHORITY]
    requester_institution: [institutional affiliation]

  # --- ACCESS PARAMETERS ---
  access:
    tier_level: TIER_0 | TIER_1 | TIER_2
    purpose_code: [code from purpose code registry, Section 10.2]
    purpose_description: [human-readable justification]
    ttl_hours: [integer — maximum access duration]
    ttl_expiry: [UTC — computed from request_timestamp + ttl_hours]
```

```
# --- SCOPE ---
scope:
  scope_type: PRODUCT | AUTHORIZATION | CUSTODY_CHAIN | DISPENSATION |
              DECISION | CLAIM | RECONCILIATION | BREAK | RECALL |
              AGGREGATE_STATISTICS
  scope_references: [list of CPO hashes, authorization IDs, event IDs,
                     break IDs, or other identifiers defining the scope]
  time_window:
    start: [UTC]
    end: [UTC]
  evidence_types_requested: [list: PAES, AES, CES, SES, DEP-H, CLM-EP,
                             ILS, PB, RECON_REPORT, ...]

# --- APPROVAL ---
approval:
  approval_required: true | false  # Tier 0 may not require approval
  approver_1:
    approver_id: [identifier]
    approval_timestamp: [UTC]
  approver_2:  # required for Tier 2
    approver_id: [identifier]
    approval_timestamp: [UTC]
  approval_conditions: [any conditions on the approval, e.g.,
                        "redact patient identifiers"]

# --- DELIVERY ---
delivery:
  delivery_format: EVIDENCE_PACK | INDIVIDUAL_ARTIFACTS | QUERY_RESULTS |
                   AGGREGATE_REPORT
  delivery_channel: [secure channel identifier]
  encryption_required: true
  delivery_timestamp: [UTC — populated at delivery]
  delivery_confirmation: [content_address of delivery receipt]

# --- POST-ACCESS ---
```

```
  post_access:
    parp_required: true | false  # true for all Tier 2; conditional for Tier 1
    parp_due_date: [UTC]
    parp_reference: [content_address of completed PARP, populated post-review]

  # --- AUDIT ---
  request_content_address: [self-referential hash]
```

Retrieval Request Lifecycle:

Stage	Event	SLA
REQUEST_SUBMITTED	Request logged as ILS record	Immediate
REQUEST_APPROVED	Approval chain completed (single for Tier 1; dual for Tier 2)	Tier 1: 4 hours; Tier 2: 2 hours (emergency) to 24 hours (routine)
RETRIEVAL_EXECUTED	Evidence artifacts retrieved from content-addressed storage; integrity verified	Per retrieval SLO (Section 9.8)
MINIMIZATION_APPLIED	Redaction, pseudonymization, and minimization applied per tier and purpose	Concurrent with retrieval
EVIDENCE_DELIVERED	Evidence pack assembled and delivered to requester	Per retrieval SLO
ACCESS_EXPIRED	TTL elapsed; access to delivered evidence governed by retention and purpose code	Automatic at TTL expiry
PARP_COMPLETED	Post-access review completed and documented	Within 5 business days of access termination

---

H.5 Retrieval Response Template

```
retrieval_response:
  response_id: [content_address]
  request_reference: [request_id from retrieval request]

  # --- RESULTS ---
  results:
    artifacts_requested: [count]
    artifacts_delivered: [count]
    artifacts_unavailable: [count, with reason codes]
    artifacts_redacted: [count — artifacts where redaction was applied]
```

```
# --- INTEGRITY ---
integrity_verification:
  artifacts_verified: [count]
  artifacts_verification_passed: [count]
  artifacts_verification_failed: [count]
  failed_artifact_list:
    - artifact_id: [content_address]
      failure_reason: [hash_mismatch | not_found | corrupted]

# --- MINIMIZATION LOG ---
minimization:
  redaction_applied: true | false
  redaction_method: [AUTOMATED | MANUAL | BOTH]
  redaction_log_reference: [content_address of redaction log]
  pseudonymization_applied: true | false
  fields_redacted: [list of field types redacted]

# --- DELIVERY ---
delivery:
  delivered_at: [UTC]
  delivery_channel: [channel identifier]
  delivery_receipt: [content_address of receipt]
  evidence_pack_manifest: [content_address of delivered pack manifest]

# --- ATTESTATION ---
attestation:
  attesting_officer: [identifier]
  attestation_statement: "The evidence delivered is complete within the
    approved scope, integrity-verified, and minimized per tier and
    purpose requirements."
  attestation_timestamp: [UTC]

response_content_address: [self-referential hash]
```

Appendix I — Offboarding Proof Bundle for Medicines, Health Products, and Clinical Decisions

I.1 Purpose

The offboarding proof bundle is the comprehensive evidence package generated when a product scope, institutional participant, or operational domain transitions out of the framework. It proves that evidence integrity was maintained through the transition and that the receiving system (or archival storage) accurately reflects the framework's evidence at the point of handover. This appendix provides the complete structure and checklist.

I.2 Offboarding Proof Bundle Manifest

```
offboarding_proof_bundle:
  bundle_id: OPB-[YYYY]-[SEQUENCE]
  offboarding_type: PRODUCT_SCOPE | PARTICIPANT | PILOT_CONCLUSION |
                    SYSTEM_DECOMMISSION | REGULATORY_DIRECTIVE
  offboarding_trigger:
    trigger_type: [per Section 13.1 trigger taxonomy]
    trigger_reference: [governance approval reference]
    trigger_timestamp: [UTC]

  # --- SCOPE ---
  scope:
    products_in_scope: [count; list of CPO references]
    authorizations_in_scope: [count; list of authorization IDs]
    custody_chains_in_scope: [count; list of chain references]
    dispensation_events_in_scope: [count]
    decision_states_in_scope: [count]
    claims_in_scope: [count, if Section 12 applicable]
    preservation_bundles_in_scope: [count; list of PB IDs]

  # --- FINAL STATE SNAPSHOT (Section 13.2) ---
  final_snapshot:
    product_evidence_snapshot:
      manifest_hash: [content_address]
      product_count: [integer]
      authenticity_state_distribution:
```

```
    VERIFIED: [count]
    UNRESOLVED: [count]
    FAILED: [count]
    NOT_ASSESSED: [count]
authorization_evidence_snapshot:
  manifest_hash: [content_address]
  authorization_count: [integer]
  validity_state_distribution:
    VALID: [count]
    EXPIRED: [count]
    SUPERSEDED: [count]
    REVOKED: [count]
    SUSPENDED: [count]
custody_evidence_snapshot:
  manifest_hash: [content_address]
  chain_count: [integer]
  chain_status_distribution:
    INTACT: [count]
    GAPPED: [count]
    COMPROMISED: [count]
    RECONSTRUCTED: [count]
safety_evidence_snapshot:
  manifest_hash: [content_address]
  ses_count: [integer]
  safety_state_distribution:
    SUFFICIENT: [count]
    INSUFFICIENT: [count]
    SUPERSEDED: [count]
    DISPUTED: [count]
reconciliation_posture_snapshot:
  manifest_hash: [content_address]
  last_reconciliation_per_type:
    - reconciliation_type: [type]
      last_execution: [UTC]
      result: ALIGNED | BREAK_DETECTED
```

```
  open_breaks_snapshot:
    open_break_count: [integer]
    breaks_by_severity:
      SEV-1: [count]
      SEV-2: [count]
      SEV-3: [count]
      SEV-4: [count]
    open_breaks_list: [content_address of detailed register]
  claim_snapshot: # if Section 12 in scope
    manifest_hash: [content_address]
    pending_claims: [count]
    open_claim_breaks: [count]
  master_snapshot_hash: [SHA-256 covering all component hashes above]

# --- FINAL RECONCILIATION (Section 13.3) ---
final_reconciliation:
  report_hash: [content_address of final reconciliation report]
  reconciliation_types_executed: [list]
  alignment_result_per_type:
    - type: [reconciliation_type]
      result: ALIGNED | BREAK_DETECTED
      break_count: [integer]
  resolved_during_final: [count of breaks resolved]
  carried_as_open: [count of breaks carried forward]
  attestation:
    attesting_officer: [identifier]
    attestation_timestamp: [UTC]

# --- LEGACY TRANSITION (Section 13.4) ---
legacy_transition:
  legacy_system_identifier: [target system ID]
  transition_manifest_hash: [content_address of legacy transition manifest]
  mapping_completeness:
    total_artifact_types: [count]
    successfully_mapped: [count]
```

```
    with_data_loss: [count]
    not_mappable: [count]
  data_loss_items:
    - artifact_type: [type]
      lost_fields: [list of field names]
      mitigation: [description — typically "archived in framework storage"]
  ingestion_verification:
    verification_timestamp: [UTC]
    record_count_match: true | false
    spot_check_result: PASS | FAIL
    verification_attestation: [content_address]

# --- OPEN BREAKS DISCLOSURE (Section 13.6) ---
open_breaks_disclosure:
  disclosure_document_hash: [content_address]
  break_count: [integer]
  governance_approval_for_offboarding_with_breaks:
    approved: true | false
    approval_reference: [governance record content_address]
    risk_acknowledgment: [content_address of risk documentation]
  accountable_parties:
    - break_id: [identifier]
      accountable_entity: [role-based identifier]
      post_offboarding_action: [continued_investigation |
                                monitoring | escalation]

# --- ARCHIVAL (Section 13.7) ---
archival:
  archival_storage_reference: [storage location identifier]
  retention_per_category:
    - evidence_category: PRODUCT_AUTHENTICITY
      retention_years: 7
    - evidence_category: AUTHORIZATION
      retention_years: 7
    - evidence_category: CUSTODY
```

```
      retention_years: 7
    - evidence_category: SAFETY_DECISION
      retention_years: 10
    - evidence_category: CLAIMS
      retention_years: 7
    - evidence_category: PRESERVATION_BUNDLES
      retention_years: INDEFINITE
    - evidence_category: OFFBOARDING_PROOF_BUNDLE
      retention_years: INDEFINITE
  post_offboarding_monitoring:
    monitoring_duration_months: 12
    monitoring_cadence: MONTHLY
    monitoring_responsible: [role-based identifier]

# --- INTEGRITY ---
integrity:
  bundle_hash: [SHA-256 of complete bundle manifest]
  all_component_hashes_verified: true | false
  verification_timestamp: [UTC]

# --- ATTESTATION ---
attestation:
  attesting_officer: [identifier]
  attestation_statement: "This offboarding proof bundle is complete
    and accurate. All evidence within scope has been captured,
    reconciled, and either transitioned to the legacy system or
    archived. Open breaks are disclosed. Data loss items are
    documented with mitigation."
  attestation_timestamp: [UTC]

bundle_content_address: [self-referential hash]
```

I.3 Offboarding Proof Bundle Checklist

#	Checklist Item	Status	Evidence Reference
1	Pre-offboarding requirements verified (all active	PASS /	[governance approval reference]

#	Checklist Item	Status	Evidence Reference
	holds resolved or transferred; governance approval obtained)	FAIL	
2	Final state snapshot generated for all evidence categories	PASS / FAIL	[master_snapshot_hash]
3	Final state snapshot integrity verified (master hash computed and confirmed)	PASS / FAIL	[verification timestamp]
4	Final reconciliation executed across all reconciliation types	PASS / FAIL	[final reconciliation report hash]
5	All breaks resolved during final reconciliation documented	PASS / FAIL	[resolved break count and references]
6	Open breaks disclosed with governance approval for offboarding	PASS / FAIL / N/A	[disclosure document hash; governance approval]
7	Legacy transition manifest generated with complete field mapping	PASS / FAIL	[transition manifest hash]
8	Data loss assessment completed for non-mappable fields	PASS / FAIL	[data loss items documentation]
9	Evidence transferred to legacy system	PASS / FAIL	[transfer records]
10	Post-transfer verification completed (record count match, spot checks)	PASS / FAIL	[verification attestation]
11	Non-transferable evidence archived per retention policy	PASS / FAIL	[archival storage reference]
12	Post-offboarding monitoring plan established	PASS / FAIL	[monitoring schedule reference]
13	Offboarding proof bundle sealed with officer attestation	PASS / FAIL	[attestation timestamp; bundle hash]
14	Bundle stored in content-addressed storage with indefinite retention	PASS / FAIL	[storage confirmation]

Appendix J — Reader Navigation Map / Reviewer Jump Table

J.1 Purpose

This navigation map helps readers locate content by role, task, or concern without reading the entire document sequentially. Each entry identifies the reader profile, the question they are trying to answer, and the section(s) that address it.

J.2 Navigation by Reader Profile

Manufacturer / Marketing Authorization Holder:

Concern	Primary Section	Supporting Appendices
How do I register products in the framework?	Section 4.1 (Canonical Product Objects)	Appendix A (A.1, A.2); Appendix B (B.1 PAES template)
What provenance evidence must I generate?	Section 4.2 (Provenance Linkage)	Appendix H (H.2 manifest template)
What happens during a recall?	Section 8.2 (Recall State Transitions)	Appendix C (C.2 BRK-PROV); Appendix F (F.2.2 Recall PB)
What are my RACI responsibilities?	Section 11.2	Appendix G (G.2 Product Authenticity RACI)

Distributor / Logistics Provider:

Concern	Primary Section	Supporting Appendices
What custody events must I log?	Section 6.1 (Custody Event Taxonomy)	Appendix C (C.4 BRK-CUST)
How do I handle storage excursions?	Section 6.2 (Storage-State Integrity)	Appendix D (PROV-003, PROV-007)
What evidence do I produce at handoff?	Section 6.3 (Handoff Workflow)	Appendix B (B.3 CES template)
How do I acknowledge a recall?	Section 8.2 (CUS_RECALL_ACK)	Appendix G (G.2 recall activities)

Pharmacy / Dispensing Entity:

Concern	Primary Section	Supporting Appendices
What must I verify before dispensing?	Section 6.4 (Dispensation Precondition Gates G1–G7)	Appendix D (DISP-001 through DISP-008)
How do I handle a blocked dispensation?	Section 6.4 (Gate failure responses); Section 7.6 (Manual confirmation)	Appendix C (all BRK types that block dispensation)
How do I document safety evidence?	Section 7.2 (Evidence Classes); Section 7.3 (Decision States)	Appendix B (B.4 SES template)
What are my RACI responsibilities?	Section 11.2	Appendix G (G.3, G.4, G.5)

Prescriber / Authorizing Clinician:

Concern	Primary Section	Supporting Appendices
How is my authorization	Section 5.1 (Authorization as Evidence);	Appendix A (A.3, A.4);

Concern	Primary Section	Supporting Appendices
modeled?	Section 5.2 (Role-Scope-Product)	Appendix B (B.2 AES template)
What happens if my credentials are restricted?	Section 5.5 (Authority Validation); Section 5.7 (Dispute Escalation)	Appendix C (C.3 BRK-AUTH-004)
How do I document an override?	Section 7.3 (DS-05); Section 7.4 (Exceptional posture)	Appendix D (SAFE-003)
What is the supersession chain?	Section 5.4 (Supersession Discipline)	Appendix A (A.4 RX states)

Hospital / Institutional Healthcare Facility:

Concern	Primary Section	Supporting Appendices
How do we implement the dispensation gates?	Section 6.4 (Gate logic)	Appendix D (DISP series); Appendix B (B.5 DEP-H template)
How do we handle clinical decision-support evidence?	Section 7.3 (Context-Bound Decision States)	Appendix B (B.4 SES template); Appendix E (EQP-009 through EQP-011)
What governance structures do we need?	Section 11.1 (Governance Body Taxonomy)	Appendix G (all RACI matrices)
How do we prepare for examiner review?	Section 14 (Examiner Readiness)	Appendix D (full checks pack); Appendix E (full query pack)

Benefit Administrator / Payer (Section 12 scope):

Concern	Primary Section	Supporting Appendices
How do I validate a claim?	Section 12.2 (Claim Evidence Gates CG-1 through CG-6)	Appendix B (B.6 CLM-EP template)
What is temporal evidence assessment?	Section 12.2 (Temporal Evidence Assessment paragraph)	Appendix E (EQP-023)
How do I handle post-payment corrections?	Section 12.6 (Adjustment, Reversal, Rebinding)	Appendix C (C.6 BRK-CLAIM); Appendix E (EQP-024)
What are my RACI responsibilities?	Section 11.2	Appendix G (G.8 Claims RACI)

Examiner / Auditor / Reviewer:

Concern	Primary Section	Supporting Appendices
What checks should I perform?	Section 14 (all subsections)	Appendix D (112 checks across 11 domains)
What queries can I run?	Section 14.9 (conceptual queries)	Appendix E (24 expanded queries)
How do I request evidence?	Section 10 (Tiered Access); Section 9.8 (Retrieval)	Appendix H (H.4 Retrieval Request template)
How do I replay a product's history?	Section 9.9 (Replay Requirements)	Appendix E (EQP-001 through EQP-003)
How do I verify an offboarding was proper?	Section 13; Section 14.8 (Offboarding Checks)	Appendix I (Offboarding Proof Bundle); Appendix D (OFFB series)

Governance Body Member:

Concern	Primary Section	Supporting Appendices
What decisions require our approval?	Section 11 (all subsections)	Appendix G (RACI — "A" column entries)
What triggers recertification?	Section 11.4 (Material Change Triggers); Section 11.5 (Recert Cadence)	Appendix D (GOVN-001, GOVN-002)
What are the liability triggers?	Section 11.6 (Liability Trigger Catalog)	Appendix D (GOVN-005)
How do we maintain no-master-key posture?	Section 11.8	Appendix D (GOVN-003); Appendix E (EQP-020)

J.3 Navigation by Task

Task	Start Here	Then Reference
Onboard a new product into the framework	Section 4.1 (CPO generation)	Section 4.2 (provenance initiation); Appendix B (B.1 PAES)
Verify product authenticity at receipt	Section 4.4 (Minimum replay requirements)	Section 6.1 (CUS_RECEIPT); Appendix D (AUTH-001 through AUTH-005)
Process a prescription for dispensation	Section 5.1 (Authorization model)	Section 6.4 (Gates); Section 7.2 (Safety evidence); Appendix B (B.2 AES, B.5 DEP-H)
Handle a dispensation gate failure	Section 6.4 (Failure responses per gate)	Section 7.6 (Manual confirmation); Appendix C (relevant break type)
Respond to a product recall	Section 8.2 (Recall state machine)	Section 6.7 (Recall custody continuity); Appendix F (F.2.2 Recall PB)
Investigate a reconciliation break	Section 9.6 (Break taxonomy and severity)	Appendix C (break code lookup); Appendix F (F.1 PB template)
Request evidence as a reviewer	Section 10 (Tiered access)	Appendix H (H.4 Retrieval request); Section 9.8 (SLOs)
Prepare for offboarding	Section 13 (all subsections)	Appendix I (Offboarding proof bundle); Appendix D (OFFB series)
Submit a reimbursement claim	Section 12.1 (Claim taxonomy)	Section 12.2 (Evidence gates); Appendix B (B.6 CLM-EP)
Correct an evidence artifact	Section 8.3 (Correction pathways)	Appendix H (H.3 EP Delta template); Section 3.9 (Correction states)

J.4 Quick Reference: Where to Find Key Concepts

Concept	Primary Definition	Extended Treatment
Product Authenticity State	Section 3.1	Appendix A (A.1)
Canonical Product Object (CPO)	Section 4.1	Appendix B (B.1 PAES template)
Dispensation Precondition Gates (G1–G7)	Section 6.4	Appendix D (DISP-001); Appendix B (B.5 DEP-H)
Proof-of-Safety State	Section 3.7	Appendix A (A.7); Section 7 (full treatment)
Context-Bound Decision State	Section 7.3	Appendix B (B.4 SES template)

Concept	Primary Definition	Extended Treatment
EP Delta	Section 3.9; Section 5.6	Appendix H (H.3 template)
Hold-Only Containment	Section 8.1	Appendix F (F.3 Hold-Set template)
Break Taxonomy	Section 9.6 (summary)	Appendix C (complete taxonomy, 41 break types)
Tiered Access (Tier 0/1/2)	Section 10.1	Section 3.12; Appendix E (query tier assignments)
Supersession Chain	Section 8.4	Section 5.4; Appendix A (all state tables)
Evidence-Linked Settlement	Section 12.2	Appendix B (B.6 CLM-EP)
Offboarding Proof Bundle	Section 13	Appendix I (full manifest and checklist)
RACI Matrices	Section 11.2	Appendix G (7 matrices)
Standard Checks Pack	Section 14 (representative)	Appendix D (112 complete checks)
Examiner Query Pack	Section 14.9 (representative)	Appendix E (24 expanded queries)

Appendix K — Minimal Glossary (Baseline-First)

K.1 Glossary Conventions

This glossary follows baseline-first vocabulary discipline: terms defined in Baselines A–E are listed with their baseline origin and used without modification. Healthcare-specific additions are listed separately with explicit justification for why no adequate baseline equivalent exists.

K.2 Baseline Terms (No Modification)

Term	Definition	Baseline Origin
Content-Addressed Storage	Storage where artifacts are identified and retrieved by the cryptographic hash of their content, ensuring integrity verification at retrieval	Baseline C
Disclosure Evidence Pack (DEP)	Cryptographically secured bundle proving disclosure assertions, with content-addressed artifact references	Baseline A
EP Delta	Incremental evidence artifact documenting a state change, preserving the prior state and linking to the new state through content-addressed references	Baselines A, C
Evidence Pack (EP)	Standardized collection of documentation, logs, and artifacts demonstrating compliance with operational requirements	Baselines B, C
Hold-Only Containment	Temporary restriction preventing state changes pending investigation or resolution; does not imply fault or violation	Baseline A
Immutable Log Segment (ILS)	Tamper-evident, hash-chained log record capturing operational events with timestamps, actor identifiers, and content-addressed integrity	Baselines A, C
Material Change Trigger	Threshold event requiring notification, re-evaluation, documentation, and potential recertification	Baselines A, B, D
No-Master-Key Posture	Design principle prohibiting single-party override capability; all material governance actions require distributed, multi-party authorization	Baselines A, B
Post-Access Review	Audit procedure following reviewer evidence retrieval to verify purpose compliance, access scope adherence, and findings documentation	Baselines C, D
Post-Access Review Pack (PARP)	Standardized documentation package produced after every Tier 2 access event and selected Tier 1 events, recording scope verification, findings, and data handling confirmation	Baselines C, D
Preservation Bundle (PB)	Sealed, content-addressed evidence collection assembled for incidents, disputes, recalls, investigations, or legal holds	Baselines A, C
Purpose Limitation	Constraint limiting evidence access and use to a specified regulatory, review, or operational function, documented through purpose codes	Baselines C, D
Recertification (Recert) Cadence	Periodic validation of control effectiveness, participant capabilities, and governance compliance	Baselines A, B, D
Tiered Supervisory Access (Tier 0/1/2)	Graduated access model: Tier 0 aggregate/statistical; Tier 1 scoped/event-triggered with pseudonymization; Tier 2	Baselines B, C, D

Term	Definition	Baseline Origin
	exceptional reveal with dual-control and mandatory post-access review	
TTL (Time-To-Live)	Temporal access window with automatic expiration; applied to reviewer access grants and proof freshness periods	Baselines C, D
Verifier Output Pack (VOP)	Standardized artifact recording proof verification results, freshness timestamps, and revocation status references for proof-carrying compliance artifacts	Baseline D

K.3 Healthcare-Specific Additions

Term	Definition	Justification
Authorization Evidence Set (AES)	Mapping construct linking prescription, authorization, or issuer legitimacy records to baseline artifact types (EP, ILS, content-addressed manifests)	No baseline equivalent for healthcare authorization evidence; adapts DEP concept to clinical authorization
Canonical Product Object (CPO)	Standardized reference record anchoring a specific product-formulation-manufacturer-batch/lot combination, serving as the identity foundation for all downstream evidence	No baseline equivalent for physical product identity; adapts registry record concept from Baseline A
Claim Evidence Gate (CG-1 through CG-6)	Structured verification checkpoint that must be satisfied before claim progression from submission to approval	Adapts DvP precondition gates from Baseline E to claim/reimbursement context
Context-Bound Decision State	Evidence record capturing the complete evidence context at the moment a clinical decision was made, enabling independent reviewer reconstruction	No baseline equivalent for clinical decision evidence preservation
Custody Evidence Set (CES)	Mapping construct linking medicine/product custody records, handoff confirmations, and storage-state logs to baseline artifact types	Adapts Ownership Evidence Set (OES) from Baseline A and Custody Evidence Pack (CEP) from Baseline B to physical product custody
Dispensation Evidence Pack (DEP-H)	Evidence pack produced at dispensation linking all precondition gate results, upstream evidence sets, and dispensation event records	Adapts settlement evidence production from Baseline E to healthcare dispensation
Dispensation Precondition Gate (G1 through G7)	Structured verification checkpoint that must be satisfied before product dispensation proceeds	Adapts DvP precondition gates from Baseline E to dispensation context
Dispensation State	Operationally evidenced condition recording the controlled release of a medicine or health product to its intended recipient	Adapts settlement state from Baseline E
Product Authenticity Evidence Set (PAES)	Mapping construct linking product identity, manufacturer origin, batch/lot references, and provenance chain to baseline artifact types	No baseline equivalent for product-level (non-securities) authenticity evidence

Term	Definition	Justification
Proof-of-Safety State	Operationally evidenced condition indicating whether sufficient safety-relevant evidence exists to support a release, dispensation, or review decision	Healthcare-specific state category not present in securities baselines
Provenance Manifest	Content-addressed document aggregating all provenance events for a product, enabling full chain verification from manufacture to current custody	Adapts content-addressed manifest from Baseline C with product-specific provenance event chaining
Safety Evidence Set (SES)	Mapping construct linking proof-of-safety records, clinical decision outputs, and safety-relevant assessment artifacts to baseline artifact types	No baseline equivalent for clinical safety evidence

K.4 Abbreviations

Abbreviation	Expansion
AES	Authorization Evidence Set
BRK	Reconciliation Break (prefix for break codes)
CES	Custody Evidence Set
CLM	Claim (prefix for claim lifecycle events)
CLM-EP	Claim/Reimbursement Evidence Pack
CPO	Canonical Product Object
CUS	Custody (prefix for custody event codes)
DEP-H	Dispensation Evidence Pack (Healthcare)
DS	Decision-level safety evidence class (prefix: DS-01 through DS-05)
EP	Evidence Pack
ILS	Immutable Log Segment
LT	Liability Trigger (prefix for trigger codes)
PAES	Product Authenticity Evidence Set
PARP	Post-Access Review Pack
PB	Preservation Bundle
PS	Product-level safety evidence class (prefix: PS-01 through PS-05)
SES	Safety Evidence Set
SEV	Severity (prefix for severity bands: SEV-1 through SEV-4)
TTL	Time-To-Live
VOP	Verifier Output Pack

Appendix L — Version Lineage, Supersession, and Revocation Templates

L.1 Purpose

This appendix provides paste-ready templates for tracking version lineage, supersession chains, and revocation records across all state categories in the framework. These templates operationalize the non-destructive preservation principle (Section 3.9, Section 8.5): every state change preserves the prior state, links to the new state through content-addressed references, and maintains a traversable version history.

L.2 Version Lineage Record Template

Every evidence artifact, authorization, product state, or safety assessment that undergoes versioning maintains a version lineage record — an ordered, content-addressed registry of all versions from genesis through current.

```
version_lineage:
  lineage_id: VL-[SUBJECT_TYPE]-[SUBJECT_REF]-[YYYY]
  subject_type: CPO | AUTHORIZATION | PRESCRIPTION | SAFETY_PROFILE |
                PROVENANCE_MANIFEST | CUSTODY_CHAIN | DECISION_STATE |
                EVIDENCE_ARTIFACT | RECONCILIATION_PROCEDURE |
                GOVERNANCE_DOCUMENT
  subject_reference: [content_address of the subject]
  subject_description: [human-readable; e.g., "Prescription RX-2026-04417"]

  versions:
    - version_number: 1
      version_hash: [content_address of version 1]
      state_at_version: [state value; e.g., RX_VALID]
      created_at: [UTC]
      created_by: [role-based identifier]
      creation_trigger: GENESIS
      ep_delta_reference: null  # no delta for genesis
      status: SUPERSEDED | CORRECTED | REVOKED | CURRENT

    - version_number: 2
      version_hash: [content_address of version 2]
      state_at_version: [state value; e.g., RX_VALID — renewed]
```

```
    created_at: [UTC]
    created_by: [role-based identifier]
    creation_trigger: RENEWAL | CORRECTION | SUPERSESSION |
                      SCOPE_MODIFICATION | FRESHNESS_REFRESH
    ep_delta_reference: [content_address of EP Delta v1→v2]
    status: SUPERSEDED | CORRECTED | REVOKED | CURRENT

  - version_number: N  # ... continued for all versions
    version_hash: [content_address]
    state_at_version: [state value]
    created_at: [UTC]
    created_by: [role-based identifier]
    creation_trigger: [trigger type]
    ep_delta_reference: [content_address of EP Delta v(N-1)→vN]
    status: CURRENT

current_reference:
  version_number: [N — the most recent non-revoked version]
  version_hash: [content_address of current version]
  state_at_current: [current state value]

lineage_integrity:
  version_count: [integer]
  chain_verified: true | false
  last_verification_timestamp: [UTC]

lineage_content_address: [self-referential hash]
```

Lineage Operating Rules:

- A new version is appended (never inserted) to the lineage.
- Each version except genesis references an EP Delta documenting the transition.
- Only one version may have status = CURRENT at any time. If the current version is revoked, status becomes REVOKED and current_reference is set to null — requiring re-authorization or re-assessment.
- Historical versions remain accessible by version_number or version_hash for examiner replay.

- Lineage integrity is verified periodically by confirming that the EP Delta chain is unbroken and that each version's content_address matches the stored artifact.

L.3 Supersession Chain Template

Supersession chains track the ordered replacement of one artifact or state by a newer version. They are a subset of version lineage focused specifically on replacement relationships.

```
supersession_chain:
  chain_id: SC-[SUBJECT_TYPE]-[SUBJECT_REF]
  subject_type: PRESCRIPTION | SAFETY_PROFILE | FORMULARY_VERSION |
                ALGORITHM_VERSION | GOVERNANCE_DOCUMENT |
                PRODUCT_SPECIFICATION | CREDENTIAL
  subject_scope: [description of what is being superseded;
                  e.g., "Prescription for Patient Q, Product Y"]

  chain_entries:
    - position: 1
      artifact_hash: [content_address of original]
      state: SUPERSEDED
      effective_from: [UTC]
      effective_until: [UTC — when superseded]
      superseded_by: [content_address of position 2]
      supersession_reason: [RENEWAL | REPLACEMENT | UPDATE |
                            REGULATORY_CHANGE | CORRECTION]
      supersession_authority: [role-based identifier]

    - position: 2
      artifact_hash: [content_address of replacement]
      state: SUPERSEDED
      effective_from: [UTC]
      effective_until: [UTC]
      superseded_by: [content_address of position 3]
      supersession_reason: [reason]
      supersession_authority: [identifier]

    - position: N  # current
```

```
    artifact_hash: [content_address of current]
    state: CURRENT
    effective_from: [UTC]
    effective_until: null  # current — no end date
    superseded_by: null
    supersession_reason: null
    supersession_authority: null

  current_position: [N]
  current_artifact_hash: [content_address of current version]
  chain_length: [integer]
  chain_content_address: [self-referential hash]
```

Supersession Chain Verification Queries:

Verification	Method	Expected Result
Chain completeness	Traverse from position 1 to N; confirm no gaps	Every position occupied; no missing entries
Linkage integrity	For each entry, confirm superseded_by matches the next position's artifact_hash	All forward pointers valid
Single current	Count entries with state = CURRENT	Exactly 1 (or 0 if current is REVOKED)
No orphans	Confirm every entry except position 1 is referenced as superseded_by from the preceding entry	No unreachable entries
Temporal consistency	Confirm effective_from of each entry ≥ effective_until of preceding entry	No temporal overlaps

---

L.4 Revocation Record Template

Revocation records document the permanent invalidation of an evidence artifact, authorization, credential, or product state. Revocation is distinct from supersession: a superseded artifact is replaced by a newer version; a revoked artifact is invalidated without automatic replacement.

```
revocation_record:
  revocation_id: REV-[SUBJECT_TYPE]-[YYYY]-[SEQUENCE]
  revoked_artifact:
    artifact_hash: [content_address of revoked artifact]
    artifact_type: [AUTHORIZATION | CREDENTIAL | PROOF_ARTIFACT |
                    PRODUCT_STATE | SAFETY_EVIDENCE | CPO]
    artifact_description: [human-readable]
    state_before_revocation: [state value immediately before revocation]
```

```
revocation_details:
  revocation_timestamp: [UTC]
  revocation_authority: [role-based identifier]
  authority_basis: CREDENTIALING_BODY_ACTION | GOVERNANCE_DECISION |
                   REGULATORY_DIRECTIVE | ENFORCEMENT_ACTION |
                   ISSUER_INITIATED | INTEGRITY_FAILURE |
                   MATERIAL_CHANGE | SAFETY_DETERMINATION
  revocation_reason: [plain-language explanation]
  revocation_evidence: [content_address of supporting evidence]

downstream_impact:
  dependent_authorizations: [count and list of authorization IDs
                             that relied on revoked artifact]
  dependent_dispensation_events: [count — completed dispensation
                                  under revoked artifact]
  dependent_claims: [count of pending or paid claims linked]
  hold_actions_triggered: [count of holds initiated on dependent items]
  notification_records:
    - notified_entity: [identifier]
      notification_timestamp: [UTC]
      notification_method: [channel]
    - ...

propagation_status:
  propagation_complete: true | false
  items_propagated: [count]
  items_pending: [count]
  propagation_completion_target: [UTC]

non_retroactivity_note: "This revocation is prospective. Prior
  verifier output logs, dispensation events, and decisions made
  in good faith under the now-revoked artifact before the
  revocation timestamp remain as historical evidence and are
  not retroactively invalidated."
```

```
revocation_record_content_address: [self-referential hash]
```

Revocation vs. Correction vs. Supersession — Decision Logic:

Situation	Appropriate Action	Template
Artifact contains factual error but remains conceptually valid	Correction — new version replaces erroneous version	EP Delta (Appendix H, H.3)
Artifact is replaced by a newer version (e.g., updated prescription, new formulary)	Supersession — new version takes over as current reference	Supersession Chain (L.3)
Artifact is permanently invalidated (e.g., credential revoked, product withdrawn, fraud detected)	Revocation — artifact invalidated; no automatic replacement	Revocation Record (L.4)
Artifact is temporarily invalid pending investigation	Suspension — hold-only containment; not revocation	Hold-Set (Appendix F, F.3)

L.5 Combined Lineage and Revocation Example

Scenario: Prescription RX-2026-04417 — lifecycle from issuance through renewal, scope modification, and eventual revocation.

Version	State	Trigger	EP Delta	Effective Period
v1	RX_VALID	Genesis (issuance by Dr. K)	None	2026-01-15 → 2026-04-15
v2	RX_VALID	Renewal (90-day extension by Dr. K)	ED-RX-04417-v1v2	2026-04-15 → 2026-07-15
v3	RX_VALID	Scope modification (quantity reduced per clinical review)	ED-RX-04417-v2v3	2026-05-20 → 2026-07-15
v4	RX_REVOKED	Revocation (Dr. K credential restriction; governance-initiated)	ED-RX-04417-v3v4	2026-06-01 → terminal

Version lineage: v1 → v2 (renewal) → v3 (scope mod) → v4 (revoked). Current reference: null (revoked). All prior versions preserved for replay. Dispensation events at v1 and v2 periods remain valid historical evidence. Pending dispensation at v3 was held at revocation; patient referred for re-authorization.

Appendix M — Scope-of-Use and Authority Matrix (Time / Location / Purpose / Issuer / Release Conditions)

M.1 Purpose

This appendix provides a comprehensive authority matrix documenting the bound categories (Section 5.3) that constrain every authorization and release action in the framework. The matrix is designed as a paste-ready reference for dispensation systems, compliance functions, and examiner verification.

M.2 Authorization Bound Matrix — Full

Bound Category	Bound Definition	Evidence Field(s)	Verification Method	Failure Response
Time Bound	Authorization valid only within defined temporal window	validity_start, validity_end, duration_limit	Timestamp comparison: dispensation_time must fall within [validity_start, validity_end]	EXPIRED state; dispensation blocked; renewal or re-authorization required
Location Bound	Authorization valid only at specified dispensation locations or jurisdictions	authorized_locations[], jurisdiction_codes[], setting_types[]	Location-match: dispensation_point.location compared against authorized_locations	Scope mismatch break (BRK-AUTH-005); dispensation blocked
Purpose Bound	Authorization valid only for specified clinical purposes or patient populations	purpose_codes[], population_restrictions[], indication_codes[]	Purpose-match: intended use compared against purpose_codes; off-label use triggers DS-05 documentation requirement	Scope mismatch; Exceptional review posture if off-label
Quantity Bound	Authorization specifies maximum quantities, refill limits, or dosage ceilings	max_quantity, max_refills, dosage_ceiling, dispensed_to_date, refills_used	Accumulation check: dispensed_to_date + current_request ≤ max_quantity; refills_used < max_refills	Quantity exceeded; dispensation blocked; new authorization required
Product Bound	Authorization specific to identified product(s); substitution governed by explicit policy	authorized_products[], substitution_policy, therapeutic_equivalence_flag	Product-match: dispensation product CPO compared against authorized_products; substitution only if policy permits	Product mismatch; dispensation blocked unless substitution policy explicitly authorizes
Channel	Authorization	authorized_channels[],	Channel-match:	Channel

Bound Category	Bound Definition	Evidence Field(s)	Verification Method	Failure Response
Bound	valid only when transmitted through recognized channels	transmission_record, channel_verification	prescription received through authorized channel (e.g., electronic prescribing network, institutional order system)	verification failure; dispensation held pending channel confirmation
Issuer Bound	Authorization valid only from issuers meeting credential and scope requirements	issuer_credential_ref, authority_type, scope_attestation, delegation_chain (if delegated)	AES verification per Section 5.5: legitimacy CONFIRMED; scope covers product and setting; credential non-revoked	Issuer legitimacy failure (BRK-AUTH-003/004); dispensation blocked

---

M.3 Release Condition Matrix

Release conditions are compound requirements that must all be satisfied before a product may be released for dispensation, transfer, or claim progression. This matrix maps release conditions to their evidence sources and verification mechanisms.

Release Conditions for Dispensation (Gates G1–G7 Expanded):

Release Condition	Evidence Source	Verification	Mandatory / Conditional
Product authenticity = VERIFIED	PAES	Complete PAES with provenance manifest COMPLETE; manufacturer identity CONFIRMED; integrity checks PASS	Mandatory for all dispensation
Authorization = VALID	AES	Authorization validity RX_VALID; issuer legitimacy ISSU_CONFIRMED; all bounds verified	Mandatory for all dispensation
Scope match confirmed	AES + dispensation parameters	Each bound category (time, location, purpose, quantity, product, channel, issuer) verified and PASS	Mandatory for all dispensation
Custody chain = INTACT	CES	No unresolved custody gaps; no unassessed excursions; most recent custody event within freshness window	Mandatory for all dispensation
Safety evidence = SUFFICIENT	SES	All required evidence classes (per Section 7.2 matrix) present and current	Mandatory for all dispensation
No active hold/recall/quarantine	Hold/recall/ quarantine state records	Product recall/quarantine/hold state = ACTIVE (no hold in effect)	Mandatory for all dispensation
Revocation check passed (optional)	VOP or revocation check	Authorization and product-reference revocation checks passed within	Conditional: mandatory where

Release Condition	Evidence Source	Verification	Mandatory / Conditional
	record	freshness window	Baseline D patterns applied

Release Conditions for Claim Progression (Gates CG-1–CG-6):

Release Condition	Evidence Source	Verification	Mandatory / Conditional
Dispensation evidence exists	DEP-H	Valid, content-addressed DEP-H referencing the dispensation event	Mandatory
Authorization valid at dispensation time	AES temporal assessment	Authorization state was RX_VALID at dispensation timestamp (not at claim submission time)	Mandatory
Product authenticity verified at dispensation	PAES temporal assessment	Authenticity state was AUTH_VERIFIED at dispensation timestamp	Mandatory
Safety evidence sufficient at dispensation	SES temporal assessment	Safety state was SAFE_SUFFICIENT at dispensation timestamp	Mandatory
No active recall at claim submission	Product state records	Product not subject to active recall at time of claim submission	Mandatory
No duplicate claim	Claim records	No prior paid claim for the same dispensation event	Mandatory

---

M.4 Authority Delegation Matrix

When authorization authority is delegated (Section 5.2), the delegation must be documented with scope constraints matching the delegator's own authority boundaries.

Delegation Attribute	Requirement	Evidence
Delegator authority verified	Delegator's own AES must show ISSU_CONFIRMED with scope covering the delegated action	Delegator AES content_address
Delegation instrument documented	Formal delegation instrument (protocol, standing order, collaborative practice agreement) recorded as content-addressed artifact	Delegation instrument content_address
Delegation scope ≤ delegator scope	Delegate's authorized scope cannot exceed delegator's scope on any bound category	Scope comparison record
Delegation temporal validity	Delegation has defined start/end dates; does not outlive delegator's own credential validity	Delegation validity_start and validity_end
Delegation revocability	Delegation can be revoked by delegator or governance body at any time; revocation takes effect immediately	Revocation mechanism documented in delegation instrument
Delegate identity verified	Delegate's credentials verified and non-revoked at each use of delegated authority	Delegate credential check at each delegated dispensation
Chain depth limit	Multi-level delegation (A → B → C) requires	Governance approval record

Delegation Attribute	Requirement	Evidence
	explicit governance approval; maximum chain depth defined by institutional policy	if chain depth > 1

Appendix N — Worked Mini-Scenario Pack (Cross-Domain)

N.1 Purpose

This appendix provides condensed cross-domain mini-scenarios demonstrating how multiple framework components interact in realistic operational situations. Each scenario is shorter than the full worked examples in Section 15 but focuses on cross-domain linkage — how evidence flows between product, authorization, custody, safety, and claim domains.

N.2 Mini-Scenario: Formulary Change Triggers Multi-Domain Cascade

Setup. Hospital H updates its formulary from version F-v12 to F-v13, effective immediately. F-v13 removes Product A from the approved formulary due to cost-effectiveness review and adds Product B as its replacement.

Cross-Domain Evidence Cascade:

Step	Domain	Event	Evidence Generated
1	Governance	Formulary change approved by Pharmacy and Therapeutics Committee; material change trigger activated	MATERIAL_CHANGE ILS record; governance approval; formulary version EP Delta (F-v12 → F-v13)
2	Safety	All SES records referencing F-v12 for Product A now reference a superseded formulary version; safety state for Product A dispensation transitions to SAFE_SUPERSEDED	Safety evidence supersession records for all active Product A SES artifacts; BRK-FRESH-002 detection
3	Authorization	Active prescriptions for Product A reviewed; prescriptions with therapeutic substitution policy = ALLOWED flagged for automatic substitution to Product B; prescriptions without substitution policy held	Authorization review records; substitution eligibility assessment per prescription
4	Dispensation	Pending dispensation requests for Product A blocked at Gate G5 (safety evidence superseded) until SES refreshed against F-v13	Gate G5 FAIL records; dispensation holds
5	Prescriber notification	Prescribers with active Product A prescriptions without substitution policy notified; re-authorization requested	Notification records; re-authorization requests
6	Claim	Pending claims for Product A dispensation events completed before formulary change: unaffected (temporal assessment — safety evidence was SUFFICIENT at dispensation time)	No claim holds; temporal assessment confirms pre-change dispensation valid
7	Resolution	Prescribers re-authorize with Product B; SES refreshed against F-v13 for Product B; dispensation gates pass	New AES for Product B prescriptions; fresh SES; dispensation proceeds

Key Insight. A single governance event (formulary change) generates evidence cascades across 5 domains. The framework's temporal assessment ensures pre-change dispensation and claims are not retroactively invalidated, while post-change dispensation is appropriately held until evidence is refreshed.

N.3 Mini-Scenario: Cold-Chain Break During Distribution Affects Downstream Dispensation and Claim

Setup. A temperature monitoring system at Distributor D detects a 6-hour cold-chain excursion affecting 200 units of Product C (a biologic requiring 2–8°C storage) during overnight storage.

Cross-Domain Evidence Cascade:

Step	Domain	Event	Evidence Generated
1	Custody	CUS_TEMP_EXCURSION detected; excursion classified as Moderate (6h, peak 14°C)	Excursion detection record; severity assessment
2	Custody	Hold-only containment applied to all 200 units	CUS_HOLD_ENTRY for 200 units
3	Provenance	Provenance manifest annotated with excursion event; provenance state remains PROV_COMPLETE but with excursion flag	Provenance manifest update
4	Safety	PS-03 (storage condition compliance) flagged as non-compliant for affected units; proof-of-safety state → SAFE_INSUFFICIENT	SES update; BRK-SAFE break for storage condition non-compliance
5	Custody	Quality assessment performed: manufacturer stability data indicates Product C tolerates ≤12h at ≤15°C without potency impact; 6h at 14°C is within tolerance	Quality assessment record (content-addressed); manufacturer stability data reference
6	Custody	Hold released based on quality assessment; excursion assessment record links to manufacturer data	CUS_HOLD_RELEASE with quality assessment evidence; excursion assessment record
7	Safety	PS-03 updated with excursion assessment result; safety state → SAFE_SUFFICIENT (with documented excursion and assessment)	SES refresh; excursion-assessed PS-03
8	Dispensation	Units released for dispensation; dispensation gates pass with note that PS-03 includes assessed excursion	Dispensation proceeds normally; DEP-H includes excursion assessment reference
9	Claim	Claims for dispensation of affected units process normally; excursion assessment evidence is part of the evidence chain	No claim impact; evidence chain complete

Key Insight. The excursion triggered appropriate containment (hold-only), but did not result in product loss because the quality assessment confirmed acceptability. The complete evidence chain — excursion detection, hold, assessment, release — is preserved and available for examiner replay.

N.4 Mini-Scenario: Credential Revocation Discovered During Claim Adjudication

Setup. Benefit Administrator B is adjudicating claim CLM-2026-11203 for dispensation of Product D. During CG-2 (Authorization Linkage) evaluation, the gate engine discovers that the prescriber's credential was revoked 2 days before the dispensation event — meaning the dispensation itself may have been unauthorized.

Cross-Domain Evidence Cascade:

Step	Domain	Event	Evidence Generated
1	Claim	CG-2 temporal assessment: prescriber credential revoked before dispensation timestamp; gate FAIL	Gate CG-2 failure record: "ISSU_REVOKED pre-dispensation"
2	Claim	Claim denied (CLM_DENIED); reason: authorization invalid at dispensation time	CLM_DENIED record with BRK-AUTH-002 reference
3	Authorization	Retroactive review triggered: all dispensation events by this prescriber in the window between credential revocation and system detection identified	BRK-AUTH-004 detection; affected dispensation inventory
4	Dispensation	All affected dispensation events flagged for post-dispensation review; patient notification assessment initiated	Post-dispensation review records; notification assessment
5	Safety	Clinical assessment of affected patients: were dispensed products appropriate regardless of prescriber credential status?	Clinical review records (Tier 1 access under PUR-SAFETY-INCIDENT)
6	Governance	Liability trigger LT-03 activated: authorization by entity with revoked credentials	LT-03 record; Preservation Bundle initiated; governance notification
7	Claim	All claims referencing this prescriber during the affected window reviewed; additional denials or adjustments as appropriate	Claim review records; CLM_DENIED or CLM_ADJUSTED for affected claims
8	Governance	Root cause investigation: why was credential revocation not detected at dispensation time? Freshness window review	Investigation report; control improvement recommendations

Key Insight. The claim adjudication process served as a secondary detection point for an authorization integrity failure. The temporal assessment correctly identified that the credential was revoked before dispensation — unlike worked example 15.6, where revocation occurred after dispensation and the claim was appropriately approved.

N.5 Mini-Scenario: Examiner Requests Cross-Domain Replay for Adverse Event Investigation

Setup. An adverse event report is received for Patient E who received Product F at Hospital H. The examiner requests a complete cross-domain replay to understand what happened.

Replay Sequence:

Replay Domain	Examiner Query	Evidence Retrieved	Tier
Product	"Show authenticity and provenance for the dispensed unit of Product F" (EQP-001, EQP-003)	PAES: AUTH_VERIFIED; provenance chain COMPLETE from manufacturer through Hospital H; no breaks detected	Tier 1
Authorization	"Show authorization lifecycle for the prescription" (EQP-004)	AES: issuer ISSU_CONFIRMED at dispensation; prescription RX_VALID; scope match confirmed; no supersession	Tier 1
Custody	"Show custody chain for this specific unit" (EQP-003 adapted)	CES: CUST_INTACT; storage conditions compliant; no excursions; handoff chain complete	Tier 1
Safety	"Show safety evidence at dispensation time" (EQP-010)	SES: SAFE_SUFFICIENT; all required evidence classes present; no alerts overridden; DS-01 contraindication check CLEAR; DS-02 interaction check CLEAR	Tier 1
Dispensation	"Show complete dispensation record"	DEP-H: all gates G1–G7 PASS; standard review posture; dispensation executed normally	Tier 1
Decision context	"Was there any clinical decision-support involvement?"	No context-bound decision state for this dispensation (standard dispensation; no alerts triggered)	Tier 1

Examiner Conclusion. Cross-domain replay confirms that all operational evidence was present, current, and consistent at dispensation time. The adverse event is not attributable to an evidence gap, authorization failure, custody compromise, or safety evidence deficiency. The adverse event investigation proceeds through clinical channels (outside framework scope) with the assurance that the operational evidence layer functioned as intended.

N.6 Mini-Scenario: Offboarding with Open Breaks

Setup. Distributor D is exiting the framework. During final reconciliation, 3 open breaks are detected: 2 BRK-FRESH-003 (stale custody evidence for products in long-term storage) and 1 BRK-PROV-006 (aggregation hierarchy break for a repackaged lot).

Offboarding Sequence:

Step	Action	Evidence
1	Final reconciliation detects 3 breaks; BRK-FRESH-003 (x2) classified SEV-4; BRK-PROV-006 classified SEV-3	Final reconciliation report with break details
2	SEV-4 breaks: custody evidence refreshed through manual	CUS_STORAGE verification

Step	Action	Evidence
	verification; breaks resolved	events; break closure records
3	SEV-3 break: aggregation investigation initiated but cannot be completed before offboarding deadline (requires manufacturer records not yet available)	Investigation partial results; manufacturer records request
4	Open breaks disclosure prepared: 1 unresolved break (BRK-PROV-006); governance approval requested for offboarding with open break	Open breaks disclosure document; risk assessment
5	Governance approves offboarding with open break; Distributor D assigned as accountable party for post-offboarding resolution	Governance approval record; accountability assignment
6	Offboarding proof bundle generated with open break disclosure; legacy transition executed	OPB manifest with open break section populated
7	Post-offboarding monitoring: break tracked in open breaks register; manufacturer records received at T+15d; break resolved	Break resolution record; open breaks register closure

Appendix O — Materiality & Escalation Matrix for Product, Authorization, Custody, and Safety Breaks

O.1 Purpose

This appendix provides a unified materiality and escalation matrix that defines — for each break domain — the thresholds that determine when a break escalates from routine handling to governance notification, Tier 2 access, preservation bundle generation, or regulatory notification. The matrix complements the break taxonomy (Appendix C) and severity classification (C.9) with escalation-specific criteria.

O.2 Materiality Thresholds by Domain

Product Authenticity and Provenance Breaks:

Escalation Level	Materiality Threshold	Trigger Examples
Routine handling	Isolated SEV-4 break; single product unit; no downstream dispensation	Minor metadata discrepancy in provenance event; timestamp precision mismatch
Enhanced investigation	SEV-3 break; or SEV-4 break recurring 3+ times in 30 days for same product category	Aggregation hierarchy gap for a repackaged lot; repeated batch/lot reference discrepancies from same source
Governance notification	Any SEV-2 break; or SEV-3 break unresolved beyond SLA; or pattern affecting 3+ products from same manufacturer	Batch/lot mismatch at receipt for narrow therapeutic index product; provenance chain hash break
Preservation Bundle + Tier 2	Any SEV-1 break; or SEV-2 break with counterfeit/substitution indicators	Manufacturer identity mismatch; duplicate unit identifier; confirmed hash chain tampering
Regulatory notification	Confirmed counterfeit detection; confirmed supply chain compromise affecting public safety	BRK-PROV-003 confirmed as counterfeit; BRK-PROV-005 confirmed as duplicate indicating parallel supply chain

Authorization and Issuer Legitimacy Breaks:

Escalation Level	Materiality Threshold	Trigger Examples
Routine handling	Isolated freshness break for low-risk authorization type; no pending dispensation	BRK-FRESH-001 for standing order review cadence slightly overdue
Enhanced investigation	Scope mismatch detected at dispensation; or delegation instrument expired without renewal	BRK-AUTH-005 minor scope variation; BRK-AUTH-007 delegation expired by <7 days
Governance notification	Revoked issuer with active prescriptions; dispensation bound to expired authorization at time of dispensation	BRK-AUTH-004 issuer credential revoked; BRK-AUTH-001 dispensation under expired authorization

Escalation Level	Materiality Threshold	Trigger Examples
Preservation Bundle + Tier 2	Dispensation under pre-dispensation revoked authorization; or credential fraud suspected	BRK-AUTH-002 confirmed; suspected fraudulent credential use
Regulatory notification	Systematic unauthorized prescribing; credential fraud confirmed	Pattern of dispensation under forged or misappropriated credentials

Custody and Storage Breaks:

Escalation Level	Materiality Threshold	Trigger Examples
Routine handling	Minor quantity discrepancy (<1%) at handoff; stale custody evidence within 2x freshness threshold	BRK-CUST-004 with 0.5% variance; BRK-CUST-006 minor staleness
Enhanced investigation	Moderate storage excursion for condition-sensitive product; unmatched handoff persisting >24h	BRK-CUST-003 moderate excursion; BRK-CUST-001 unresolved >24h
Governance notification	Product identity mismatch at receipt; unauthorized actor in custody chain; critical storage excursion	BRK-CUST-005; BRK-CUST-002; severe/critical excursion
Preservation Bundle + Tier 2	Confirmed product substitution; deliberate custody chain manipulation	BRK-CUST-005 confirmed substitution; BRK-CUST-002 unauthorized access with custody modification
Regulatory notification	Confirmed product diversion; systematic custody integrity failure	Pattern of unauthorized custody events; confirmed diversion network

Safety Evidence Breaks:

Escalation Level	Materiality Threshold	Trigger Examples
Routine handling	Supplementary evidence class stale; minor formulary version lag for non-critical product	BRK-SAFE-002 minor update for standard product
Enhanced investigation	Required evidence class absent for completed dispensation; safety alert overridden without documentation	BRK-SAFE-001 for DS-01 or DS-02; BRK-SAFE-003
Governance notification	Pattern of undocumented overrides from same dispensation point; deprecated algorithm version affecting multiple decisions	BRK-SAFE-003 recurrent; BRK-SAFE-004 with error-flagged version
Preservation Bundle + Tier 2	Conflicting safety evidence classes unresolved; patient safety incident linked to safety evidence gap	BRK-SAFE-005 with hold-only containment; adverse event correlated with BRK-SAFE-001
Regulatory notification	Systematic safety evidence failures suggesting institutional control breakdown	Pattern of dispensation without required safety checks across multiple products

O.3 Escalation Response Matrix (Unified)

Escalation Level	Notification Target	SLA	Required Actions	Evidence Produced
Routine handling	Operational management only	Per break severity SLA (Appendix C, C.10)	Standard break resolution workflow	Break record; resolution record; closure record
Enhanced investigation	Operational management + surveillance function	Within 24h of detection	Dedicated investigation assignment; root cause analysis; control review	Investigation report; RCA; control improvement recommendations
Governance notification	Governance body (Steering Committee or Change Control Board)	Within 8h for SEV-2; within 2h for SEV-1	Governance briefing; resource allocation; coordination with affected parties; potential recertification assessment	Governance notification record; briefing materials; action plan
Preservation Bundle + Tier 2	Governance body + regulatory liaison function	Tier 2 access within 2h (emergency) to 24h (standard); PB initiated immediately	Full investigation under Tier 2 access; preservation of all evidence; coordination with regulatory liaison	Preservation Bundle per Appendix F; Tier 2 access records; PARP
Regulatory notification	External regulatory authority per institutional policy	Per institutional regulatory notification procedures	Regulatory communication; evidence production per regulatory request; ongoing coordination	Regulatory notification record; evidence production records; correspondence

O.4 Recurrence Escalation Rules

Recurrence of the same break type within a defined window triggers automatic escalation regardless of individual break severity.

Recurrence Pattern	Auto-Escalation	Rationale
Same break code, same scope, 3+ times in 30 days	Escalate one level above individual break handling	Pattern suggests systemic issue, not isolated incident
Same break code, different scope, 5+ times in 30 days	Escalate to governance notification	Broad pattern suggests control framework weakness
Any SEV-2+ break from same participant/entity, 3+ times in 90 days	Governance review + recertification assessment	Recurring material breaks indicate participant control deficiency
Any break type, same product category, 10+ times in 90 days	Governance review + product-category-level assessment	Category-wide issue requiring systemic investigation
Tier 2 access for same	Governance exception-creep review	Repeated Tier 2 access may

Recurrence Pattern	Auto-Escalation	Rationale
participant, 3+ times in 90 days	per Baseline D (Section 2.5)	indicate surveillance creep or persistent control failures

---

O.5 Escalation Decision Tree (Paste-Ready)

```
Break detected
  │
  ├─ Assess individual severity per Appendix C taxonomy
  │    └─ Apply aggravating/mitigating factors per C.9
  │
  ├─ Check recurrence pattern
  │    └─ If recurrence threshold met → auto-escalate per O.4
  │
  ├─ Determine materiality per O.2 domain-specific thresholds
  │    └─ Map to escalation level
  │
  ├─ Execute response per O.3 unified matrix
  │    ├─ Routine → standard resolution workflow
  │    ├─ Enhanced → dedicated investigation
  │    ├─ Governance → briefing + action plan
  │    ├─ PB + Tier 2 → full investigation + preservation
  │    └─ Regulatory → external notification + coordination
  │
  └─ Document escalation decision in break record
       └─ Include: severity, materiality assessment, recurrence check,
          escalation level determined, rationale
```

Appendix P — Optional Claim / Reimbursement Linkage Templates (Only if Section 12 Is Included)

P.1 Purpose and Conditionality

This appendix is included only when Section 12 (Financially Consequential Workflows) is in scope. It provides paste-ready linkage templates connecting claim/reimbursement events to their underlying product, authorization, dispensation, and safety evidence. These templates operationalize the evidence-linked settlement confirmation principle from Baseline E: financially consequential actions should not proceed when evidence states are materially unresolved.

P.2 Claim-to-Dispensation Linkage Template

Every claim must be traceable to a specific dispensation event through content-addressed references. This template defines the minimum linkage structure.

```
claim_dispensation_linkage:
  linkage_id: CDL-[CLAIM_ID]
  claim_reference:
    claim_id: [identifier]
    claim_submission_timestamp: [UTC]
    claimant_reference: [pseudonymized]
  dispensation_reference:
    dispensation_event_id: [content_address]
    dispensation_timestamp: [UTC]
    dep_h_manifest: [content_address of DEP-H]
  upstream_evidence_chain:
    paes_at_dispensation:
      manifest_hash: [content_address]
      authenticity_state: [AUTH_ value at dispensation time]
    aes_at_dispensation:
      manifest_hash: [content_address]
      issuer_legitimacy: [ISSU_ value at dispensation time]
      prescription_validity: [RX_ value at dispensation time]
    ces_at_dispensation:
      manifest_hash: [content_address]
      custody_state: [CUST_ value at dispensation time]
    ses_at_dispensation:
      manifest_hash: [content_address]
```

```
    safety_state: [SAFE_ value at dispensation time]
  temporal_assessment:
    assessment_method: STATE_AT_DISPENSATION_TIME
    assessment_timestamp: [UTC — when temporal assessment was performed]
    authorization_valid_at_dispensation: true | false
    product_verified_at_dispensation: true | false
    safety_sufficient_at_dispensation: true | false
    custody_intact_at_dispensation: true | false
  gate_results:
    CG-1_dispensation_evidence: PASS | FAIL
    CG-2_authorization_linkage: PASS | FAIL
    CG-3_product_authenticity: PASS | FAIL
    CG-4_safety_evidence: PASS | FAIL
    CG-5_no_active_recall: PASS | FAIL
    CG-6_no_duplicate: PASS | FAIL
  linkage_integrity:
    all_references_verified: true | false
    verification_timestamp: [UTC]
  linkage_content_address: [self-referential hash]
```

P.3 Claim Adjustment Linkage Template

When a previously paid claim is adjusted (CLM_ADJUSTED) or reversed (CLM_REVERSED), the adjustment must be linked to the upstream evidence change that triggered it.

```
claim_adjustment_linkage:
  linkage_id: CAL-[CLAIM_ID]-[ADJUSTMENT_SEQUENCE]
  original_claim:
    claim_id: [identifier]
    original_status: CLM_PAID
    original_payout_amount: [value]
    original_payout_timestamp: [UTC]
  adjustment:
    adjustment_type: CLM_ADJUSTED | CLM_REVERSED
    adjustment_amount: [value — positive for underpayment correction,
                        negative for overpayment recovery, full amount
                        for reversal]
```

```
  adjustment_timestamp: [UTC]
  adjustment_reason_code: AUTH_REVOKED_PRE_DISPENSATION |
                          PRODUCT_RECALLED | DUPLICATE_DETECTED |
                          PRICING_ERROR | EVIDENCE_CORRECTION |
                          FRAUD_DETERMINATION
  adjustment_reason_description: [plain-language]
upstream_trigger:
  trigger_type: AUTHORIZATION_REVOCATION | PRODUCT_RECALL |
                DISPENSATION_CORRECTION | EVIDENCE_INTEGRITY_FAILURE |
                DUPLICATE_DETECTION | EXTERNAL_AUDIT_FINDING
  trigger_event_reference: [content_address of triggering event —
                           e.g., revocation record, recall notification,
                           correction EP Delta]
  trigger_timestamp: [UTC — when the upstream change occurred]
  time_gap_trigger_to_adjustment: [duration — time between upstream
                                  change and adjustment execution]
approval:
  approval_authority: [role-based identifier]
  approval_chain:
    - approver: [identifier]
      timestamp: [UTC]
    - approver: [identifier]  # second approver for material adjustments
      timestamp: [UTC]
  legal_or_contractual_basis: [reference to contractual provision or
                              institutional policy authorizing adjustment]
recovery: # populated if adjustment creates recovery obligation
  recovery_amount: [value]
  recovery_initiated: true | false
  recovery_reference: [recovery tracking identifier]
  recovery_status: INITIATED | IN_PROGRESS | COMPLETED | WRITTEN_OFF
rebinding: # populated if evidence corrected (not invalidated)
  original_evidence_reference: [content_address of pre-correction evidence]
  corrected_evidence_reference: [content_address of post-correction evidence]
  ep_delta_reference: [content_address of correction EP Delta]
linkage_content_address: [self-referential hash]
```

P.4 Claim Open Breaks Register Template

The claim open breaks register tracks all unresolved breaks in the claim/reimbursement domain, adapted from Baseline E's settlement open breaks register.

```
claim_open_breaks_register:
  register_id: COBR-[YYYY]-[PERIOD]
  period:
    start: [UTC]
    end: [UTC]
  summary:
    total_open_breaks: [integer]
    breaks_by_type:
      BRK-CLAIM-001: [count]
      BRK-CLAIM-002: [count]
      BRK-CLAIM-003: [count]
      BRK-CLAIM-004: [count]
      BRK-CLAIM-005: [count]
      BRK-CLAIM-006: [count]
    breaks_by_severity:
      SEV-1: [count]
      SEV-2: [count]
      SEV-3: [count]
      SEV-4: [count]
    oldest_open_break_age_days: [integer]
    breaks_exceeding_sla: [count]
  entries:
    - break_id: [identifier]
      break_code: [BRK-CLAIM-NNN]
      severity: [SEV-N]
      detected_at: [UTC]
      age_days: [integer]
      sla_status: WITHIN_SLA | SLA_BREACHED
      affected_claim_id: [identifier]
      affected_amount: [value]
      assigned_to: [role-based identifier]
```

```
    investigation_status: PENDING | IN_PROGRESS | AWAITING_EVIDENCE
    resolution_target_date: [UTC]
  - ... [repeated for each open break]
register_content_address: [self-referential hash]
register_generated_at: [UTC]
```

Register Maintenance Rules:

Rule	Requirement
Update cadence	Updated at each claim reconciliation cycle and whenever a break is detected or resolved
Aging escalation	Breaks exceeding SLA trigger automatic governance notification per Appendix O
Offboarding requirement	Register must show zero open breaks — or governance-approved exception — before claim scope offboarding (Section 13.6)
Examiner accessibility	Register retrievable through EQP-012 (adapted for claims); Tier 0 for aggregate counts; Tier 1 for individual break details

---

P.5 Claim Evidence Completeness Scorecard Template

For periodic reporting and governance review, the claim evidence completeness scorecard summarizes the evidence quality posture across claim populations.

Metric	Calculation	Target	Reporting Cadence
Gate pass rate (overall)	Claims where all CG gates passed / Total claims validated	≥98%	Monthly
Gate pass rate per gate (CG-1 through CG-6)	Claims passing each specific gate / Total claims evaluated at that gate	≥99% per gate	Monthly
Temporal assessment accuracy	Claims where temporal assessment correctly evaluated state at dispensation time / Total temporal assessments	100%	Quarterly (sample-based)
Adjustment rate	CLM_ADJUSTED + CLM_REVERSED / Total CLM_PAID	<2% (target varies by institutional context)	Monthly
Open break aging	Average age of open claim breaks in days	<10 days	Monthly
Recovery completion rate	Recovery COMPLETED / Total recovery INITIATED	≥90% within 90 days	Quarterly
Duplicate detection rate	Duplicates detected before payment / Total duplicates identified (pre + post payment)	≥95%	Quarterly

---

Appendix Q — Proof-Based Minimization and Verifier Output Templates

Q.1 Purpose

This appendix provides templates for proof-based verification artifacts where Baseline D's programmable privacy patterns are applied. These templates enable bounded verification — confirming operational states without exposing underlying evidence — through Verifier Output Packs (VOPs) and minimized disclosure records.

Q.2 Verifier Output Pack (VOP) Template — Healthcare Application

The VOP records the result of a proof-based verification for a healthcare operational state. It adapts the VOP structure from Baseline D (Section 7.3) to healthcare evidence domains.

```
verifier_output_pack:
  vop_id: [content_address]
  verification_subject:
    subject_type: PRODUCT_AUTHENTICITY | ISSUER_LEGITIMACY |
                  PRESCRIPTION_VALIDITY | CUSTODY_INTEGRITY |
                  SAFETY_SUFFICIENCY | RECALL_STATUS |
                  CLAIM_GATE_COMPLIANCE
    subject_reference: [content_address of the subject being verified]
  claim_asserted:
    claim_type: [e.g., "Product authenticity state = VERIFIED" or
                "Issuer holds prescribing authority for product
                 category X within jurisdiction Y"]
    claim_bounded: true  # always true — claims are bounded assertions,
                         # not raw attribute disclosures
  verification_result:
    result: PASS | FAIL | STALE | REVOKED
    result_timestamp: [UTC]
    verifier_id: [pseudonymized or role-based identifier of verifying
                  component]
  freshness:
    proof_generation_timestamp: [UTC]
    validity_window_end: [UTC]
    freshness_status: CURRENT | EXPIRING | EXPIRED
```

```
  revocation:
    revocation_check_timestamp: [UTC]
    revocation_list_version: [reference to revocation list consulted]
    revocation_status: CLEAR | REVOKED | UNAVAILABLE
  evidence_mapping:
    evidence_pack_references:
      - pack_type: [PAES | AES | CES | SES | DEP-H]
        manifest_hash: [content_address]
    tier_level_of_output: TIER_0 | TIER_1
      # VOPs are Tier 0 or Tier 1 outputs by design;
      # Tier 2 accesses the underlying evidence directly
  disclosure_minimization:
    raw_attributes_exposed: NONE
      # VOPs assert bounded claims; no raw institutional,
      # patient, or commercial data exposed
    minimization_method: PROOF_CARRYING_ARTIFACT |
                         SELECTIVE_DISCLOSURE | RANGE_PROOF |
                         PASS_FAIL_ATTESTATION
  integrity:
    vop_content_address: [self-referential hash]
    stored_as: ILS  # per Baseline D convention
```

Q.3 VOP Application Matrix — Healthcare Verification Scenarios

Verification Scenario	Claim Asserted	Underlying Evidence (Not Exposed)	VOP Output (Exposed)
Product authenticity at dispensation	"Product authenticity state = VERIFIED for CPO [reference]"	Complete PAES: manufacturer credential, provenance manifest, integrity checks	PASS/FAIL + freshness status + revocation status
Issuer authority for product category	"Issuer holds authority for [product category] in [jurisdiction]"	Full issuer credential, license details, scope attestation, practice address	PASS/FAIL + freshness status
Prescription validity at dispensation	"Prescription [reference] validity = VALID at [timestamp]"	Full prescription record, issuer AES, scope details, patient reference	PASS/FAIL + freshness status + revocation status
Custody chain integrity	"Custody chain INTACT for product [reference]"	Complete custody event chain, storage condition logs, handoff records, excursion details	PASS/FAIL + chain event count + last event timestamp
Safety evidence sufficiency	"Safety evidence SUFFICIENT for	All PS and DS evidence classes, clinical decision-	PASS/FAIL + evidence class count +

Verification Scenario	Claim Asserted	Underlying Evidence (Not Exposed)	VOP Output (Exposed)
	dispensation [reference]"	support outputs, patient parameters	freshness status
Recall status clearance	"Product [reference] not subject to active recall"	Product recall/hold records, recall scope determinations, batch/lot linkage	PASS/FAIL (ACTIVE or RECALLED)
Claim gate compliance	"All CG gates passed for claim [reference]"	Dispensation evidence, authorization temporal assessment, full evidence linkage chain	PASS/FAIL per gate + overall PASS/FAIL

Reviewer Interaction with VOPs:

- At **Tier 0**, reviewers see aggregate VOP statistics: pass rates, freshness compliance percentages, revocation check success rates — no individual VOP detail.
- At **Tier 1**, reviewers access individual VOP records for specific products, authorizations, or dispensation events — seeing the bounded claim, result, freshness, and revocation status, but not the underlying evidence.
- At **Tier 2**, reviewers bypass the VOP layer and access the underlying evidence directly under standard Tier 2 controls.

Q.4 Minimized Disclosure Record Template

When a reviewer query can be answered through a minimized disclosure — providing less detail than full Tier 1 access while providing more than a simple VOP PASS/FAIL — a minimized disclosure record is generated.

```
minimized_disclosure_record:
  record_id: [content_address]
  query_reference: [retrieval_request_id that triggered this disclosure]
  disclosure_tier: TIER_1_MINIMIZED
  purpose_code: [from purpose code registry]
  ttl: [hours]
  disclosed_fields:
    - field_category: PRODUCT_IDENTITY
      disclosed: product_category, batch_lot_reference, authenticity_state
      withheld: manufacturer_commercial_terms, pricing, supply_chain_details
    - field_category: AUTHORIZATION
      disclosed: authorization_type, validity_state, scope_summary
      withheld: prescriber_name, license_number, practice_address
    - field_category: CUSTODY
```

```
      disclosed: chain_status, event_count, last_event_type,
last_event_timestamp
      withheld: custodian_commercial_identity, facility_address,
transport_details
    - field_category: SAFETY
      disclosed: safety_state, evidence_class_presence (PS/DS), override_flag
      withheld: patient_parameters, clinical_notes, raw_decision_inputs
    - field_category: CLAIM
      disclosed: claim_status, gate_results_summary, payout_status
      withheld: patient_identity, pricing_details, benefit_plan_specifics
  minimization_attestation:
    attesting_officer: [identifier]
    attestation: "Only fields necessary for the documented purpose
      have been disclosed. Withheld fields are not relevant to the
      review purpose and have been excluded per minimization
      discipline."
    attestation_timestamp: [UTC]
  record_content_address: [self-referential hash]
```

Q.5 Stale-Proof and Failed-Proof Handling Templates

When a VOP returns STALE, REVOKED, or FAIL, structured handling templates ensure consistent response.

VOP Result	Handling Template	Default Action	Escalation Path
PASS	No action template needed	Operation proceeds; VOP stored as evidence	None
STALE	Stale-proof refresh workflow	Block dependent operation; initiate re-verification; if re-verification PASS → proceed; if FAIL → escalate	Tier 1 if re-verification unavailable within SLA
REVOKED	Revoked-proof containment workflow	Block dependent operation; hold-only containment; identify dependent actions	Tier 1 immediate; Tier 2 if enforcement indicator
FAIL	Failed-proof investigation workflow	Block dependent operation; hold-only containment; investigation of failure cause	Tier 1; Tier 2 if pattern detected or safety implication
UNAVAILABLE (revocation check unreachable)	Conservative-fail workflow per Baseline D	Treat as FAIL; block dependent operation; hold-only pending revocation service restoration	Tier 1 after grace period per Baseline D

Appendix R — Cross-Border Portability and Conflict-of-Process Mini-Scenarios

R.1 Purpose and Conditionality

This appendix is included because cross-border scenarios — medicines manufactured in one jurisdiction, distributed in another, dispensed in a third — are operationally common even if the framework's primary scope is domestic. These mini-scenarios illustrate how the framework's evidence artifacts can be assessed for portability and where conflict-of-process issues arise. No cross-border regulatory framework is proposed or assumed; all scenarios use "alignment objectives" framing.

R.2 Mini-Scenario: Imported Medicine — Provenance Evidence from Foreign Manufacturer

Setup. Hospital H in Jurisdiction A receives Product G manufactured by Manufacturer M in Jurisdiction B. Product G has provenance evidence generated under Jurisdiction B's product tracking system, which uses different evidence formats and content-addressing standards than this framework.

Conflict-of-Process Points:

Issue	Framework Requirement	Jurisdiction B Reality	Resolution Approach
Provenance manifest format	Content-addressed manifest per Section 4.3	Jurisdiction B uses proprietary XML serialization format without content addressing	Mapping layer: import Jurisdiction B provenance events into framework manifest structure; generate content addresses at import; document format conversion in provenance annotation
Manufacturer credential verification	AES with issuer legitimacy ISSU_CONFIRMED per Section 5.5	Jurisdiction B credentials use different credentialing standards and revocation mechanisms	Equivalence assessment: document whether Jurisdiction B credentialing meets alignment objectives; if equivalent, generate AES with equivalence_assessed flag; if not equivalent, manufacturer identity state = ISSU_UNVERIFIED pending supplemental verification
Storage condition evidence format	Continuous condition logs per Section 6.2	Jurisdiction B requires only periodic batch attestation, not continuous monitoring	Evidence gap documented: CES annotated with "storage_monitoring = PERIODIC_ATTESTATION (Jurisdiction B standard)"; institutional quality function assesses acceptability; if accepted, provenance state PROV_COMPLETE with annotation; if not, PROV_PARTIAL
Custody chain	CUS_HANDOFF from	Border transit	Border transit documented as explicit

Issue	Framework Requirement	Jurisdiction B Reality	Resolution Approach
continuity at border	Jurisdiction B entity to Jurisdiction A importer	may introduce custody gap (customs hold, inspection, repackaging for local labeling)	custody events: CUS_HANDOFF → CUS_HOLD_ENTRY (customs) → CUS_HOLD_RELEASE → CUS_RECEIPT by importer; any gaps documented per BRK-PROV-001 handling

Evidence Artifacts Produced:

- Provenance manifest with cross-border annotation and format conversion documentation.
- AES with equivalence assessment flag for foreign manufacturer credential.
- CES with border transit custody events explicitly documented.
- Quality assessment record documenting institutional acceptance of foreign storage evidence standard.

R.3 Mini-Scenario: Prescription Issued in Jurisdiction A, Dispensation in Jurisdiction B

Setup. Patient P holds a prescription issued by Dr. K in Jurisdiction A. Patient P travels to Jurisdiction B and requests dispensation at Pharmacy Q. The prescription references Dr. K's credentials under Jurisdiction A's credentialing system.

Conflict-of-Process Points:

Issue	Framework Requirement	Conflict	Resolution Approach
Issuer legitimacy verification	AES with ISSU_CONFIRMED per Jurisdiction B standards	Jurisdiction B cannot verify Jurisdiction A credentials directly	Pharmacy Q treats authorization as ISSU_UNVERIFIED; dispensation blocked at Gate G2; escalation pathway: Pharmacy Q contacts Jurisdiction A credentialing body (if mutual recognition exists) or refers patient to local prescriber
Prescription scope validity	Location bound: authorized_locations must include Jurisdiction B	Prescription was issued with Jurisdiction A locations only	Scope mismatch detected (BRK-AUTH-005); dispensation blocked; resolution: prescriber issues cross-jurisdiction authorization amendment, or local prescriber issues new prescription
Product equivalence	Product bound: authorized_products may reference Jurisdiction A product identifiers	Product available in Jurisdiction B may have different product identifier, different formulation brand, or different packaging	Product-match verification requires cross-reference between Jurisdiction A product identifier and Jurisdiction B equivalent; therapeutic substitution policy evaluated

Issue	Framework Requirement	Conflict	Resolution Approach
Safety evidence portability	SES references Jurisdiction A formulary and interaction databases	Jurisdiction B uses different formulary and interaction data sources	Safety evidence regenerated against Jurisdiction B sources at Jurisdiction B dispensation point; SES refreshed; new DS-01 and DS-02 generated locally

Key Insight. Cross-border prescription portability is not automatic within the framework. Each bound category must be independently verified against the dispensation jurisdiction's requirements. The framework does not assert that cross-border dispensation should be permitted — it provides the evidence architecture to document what was verified, what was not, and what gaps exist.

R.4 Mini-Scenario: Recall Notification Crossing Jurisdictional Boundaries

Setup. Manufacturer M in Jurisdiction A issues a recall for Product H, Batch LOT-2026-1200. Product H was distributed to Distributors in Jurisdictions A, B, and C. Each jurisdiction has different recall notification requirements and response timelines.

Cross-Border Recall Evidence Challenges:

Challenge	Framework Response
Different recall notification formats across jurisdictions	Framework recall notification record (Section 8.2) serves as the canonical notification; jurisdiction-specific formatted notifications generated as translations with linkage to the canonical record
Different acknowledgment SLAs across jurisdictions	CUS_RECALL_ACK tracked per custody holder with jurisdiction-specific SLA notation; SLA compliance assessed per jurisdiction
Different disposition requirements (Jurisdiction B requires destruction; Jurisdiction C permits return to manufacturer)	Disposition events (CUS_DESTRUCTION or CUS_RETURN) documented per jurisdiction-specific requirement; custody chain reflects actual disposition with jurisdiction-specific regulatory reference
Consolidated recall closure requires cross-jurisdiction scope reconciliation	Recall closure report aggregates responses from all jurisdictions; each jurisdiction's affected units tracked separately; consolidated scope shows total units in scope vs. total accounted for

Evidence Artifacts Produced:

- Canonical recall notification record with jurisdiction-specific translation references.
- Per-jurisdiction CUS_RECALL_ACK tracking with jurisdiction-specific SLA notation.
- Per-jurisdiction disposition evidence (destruction or return) with regulatory reference.
- Consolidated recall closure report with cross-jurisdiction scope reconciliation.

Appendix S — Confidence / Corroboration Bands for Reviewer Use

S.1 Purpose

When reviewers assess evidence artifacts, they encounter varying levels of evidence strength. This appendix defines confidence and corroboration bands — structured categories that help reviewers calibrate their assessment without making legal determinations. Confidence bands describe the strength of individual evidence artifacts; corroboration bands describe the alignment across multiple independent evidence sources.

S.2 Confidence Bands for Individual Evidence Artifacts

Band	Label	Definition	Applicable When	Reviewer Action
CB-1	High Confidence	Evidence artifact is content-addressed, integrity-verified, within freshness window, generated by a conformance-tested source, and consistent with related artifacts	PAES complete with provenance COMPLETE and all integrity checks PASS; AES with ISSU_CONFIRMED and currency within freshness; SES with all required classes present and current	Standard reliance; no additional verification needed for the specific evidence dimension
CB-2	Moderate Confidence	Evidence artifact is present and integrity-verified but has one or more qualification: approaching freshness expiry, generated by a source not yet conformance-tested, or minor inconsistency with related artifact that does not rise to a reconciliation break	AES where freshness status = EXPIRING; CES where storage condition monitoring used periodic attestation rather than continuous; VOP result PASS but revocation list version is one behind current	Noted qualification; reviewer may proceed but should document the qualification in review findings
CB-3	Low Confidence	Evidence artifact is present but has material qualifications: exceeds freshness window, source conformance not verified, format conversion applied (cross-border import), or partial completeness	AES where freshness EXPIRED; provenance manifest PARTIAL with documented gap; cross-border evidence with equivalence_assessed flag but equivalence not confirmed	Enhanced scrutiny; reviewer should request supplemental evidence or escalate to Tier 1 investigation if relying on this evidence for a material determination
CB-4	Insufficient	Evidence artifact is absent, integrity-failed, or fundamentally incomplete;	PAES missing for dispensed product; CES with CUST_COMPROMISED	Evidence does not support operational state;

Band	Label	Definition	Applicable When	Reviewer Action
		cannot support the operational state it is supposed to evidence	status; AES with ISSU_REVOKED; VOP result FAIL	hold-only containment or denial (depending on context); break generated

---

S.3 Corroboration Bands for Cross-Source Alignment

Band	Label	Definition	Applicable When
CORR-1	Fully Corroborated	Multiple independent evidence sources agree on the operational state; no source contradicts; all sources within freshness	Product authenticity confirmed by manufacturer provenance AND custody chain verification AND receiving entity independent check
CORR-2	Substantially Corroborated	Primary evidence source confirmed; one or more secondary sources support but with minor qualification (freshness lag, format difference)	AES confirms issuer legitimacy; credentialing body reference supports but revocation list is one version behind
CORR-3	Partially Corroborated	Primary evidence source confirmed; but one or more expected secondary sources are absent or inconclusive	Provenance manifest COMPLETE but storage condition evidence available only as periodic attestation (not continuous monitoring); manufacturer identity confirmed but through imported credential with equivalence assessment
CORR-4	Uncorroborated	Single evidence source only; no independent corroboration available	Product authenticity based solely on packaging inspection without electronic provenance verification; authorization based solely on paper prescription without issuer credential verification
CORR-5	Contradicted	Two or more evidence sources produce conflicting assessments of the same operational state	Product CPO indicates Batch A; custody chain receipt indicates Batch B; or issuer credential shows CONFIRMED while revocation registry shows REVOKED

Reviewer Application Guidance:

- CORR-1 and CORR-2 support standard operational reliance.
- CORR-3 warrants documented qualification in review findings; may be acceptable for lower-risk operational decisions.
- CORR-4 should trigger enhanced scrutiny; single-source reliance for high-impact decisions (dispensation of narrow therapeutic index products, high-value claim approval) requires documented justification.
- CORR-5 triggers DISPUTED state per the applicable state taxonomy (Section 3); hold-only containment; reconciliation break generated; investigation per Appendix C break handling.

S.4 Confidence-Corroboration Cross-Reference

	CORR-1 (Fully)	CORR-2 (Substantially)	CORR-3 (Partially)	CORR-4 (Uncorroborated)	CORR-5 (Contradicted)
CB-1 (High)	Strongest posture; standard reliance	Strong posture; note minor secondary qualification	Adequate for routine decisions; document gap	Unusual — high-confidence single source warrants investigation of missing corroboration	Immediate investigation; break generated
CB-2 (Moderate)	Good posture; note primary qualification	Acceptable; document qualifications	Enhanced scrutiny recommended	Document single-source reliance with justification	Hold-only; investigation
CB-3 (Low)	Unusual combination; investigate why corroboration is strong but primary evidence weak	Review secondary sources for compensating strength	Marginal; consider hold or supplemental evidence request	Insufficient for material decisions; hold recommended	Immediate hold; SEV-2+ break
CB-4 (Insufficient)	N/A — absent/failed primary evidence	N/A	N/A	Break generated regardless	Break generated; SEV-1 if contradicted and absent

Appendix T — Performance and SLA / SLO Reference Tables

T.1 Purpose

This appendix consolidates all performance targets, service level agreements (SLAs), and service level objectives (SLOs) referenced throughout the framework into a single reference. Targets are operational alignment objectives, not binding commitments; institutional participants calibrate actual targets through governance processes.

T.2 Evidence Retrieval SLOs

Request Type	Target Response Time	Escalation if Exceeded
Standard examiner query (single product/authorization/event)	≤48 hours	Governance notification at 72 hours
Comprehensive review (multi-product, cross-domain)	≤5 business days	Governance notification at 7 business days
Emergency retrieval (safety incident, active recall, regulatory demand)	≤4 hours	Immediate governance and regulatory notification if exceeded
Dispute-related evidence production (per party)	≤48 hours	Dispute authority notified at 72 hours
Offboarding evidence production	Per offboarding timeline (typically ≤30 days)	Governance review if timeline at risk

---

T.3 Reconciliation Execution SLOs

Reconciliation Type	Default Cadence	Maximum Acceptable Delay
Provenance-Custody Alignment	Continuous alerts; daily batch	24 hours beyond scheduled batch
Authorization-Dispensation Alignment	At each dispensation; daily batch	Dispensation: real-time; batch: 24 hours
Safety Evidence Currency	Per institutional cadence (alignment: daily for high-risk)	48 hours beyond scheduled cycle
Claim-Evidence Alignment	At submission; at adjudication	24 hours beyond submission
Aggregate Holdings Reconciliation	Weekly batch	7 days beyond scheduled batch
Offboarding Reconciliation	At initiation and completion	Per offboarding timeline

---

T.4 Break Resolution SLAs

Break Severity	Containment SLA	Investigation SLA	Full Resolution SLA
SEV-1 (Critical)	≤15 minutes	≤48 hours	Case-dependent; governance oversight

Break Severity	Containment SLA	Investigation SLA	Full Resolution SLA
SEV-2 (High)	≤1 hour	≤5 business days	≤10 business days
SEV-3 (Moderate)	≤4 hours	≤10 business days	≤30 business days
SEV-4 (Low)	Next reconciliation cycle	≤30 business days	≤30 business days

T.5 Tiered Access SLAs

Access Action	SLA	Escalation
Tier 1 approval	≤4 hours from request	Auto-escalation to secondary approver at 8 hours
Tier 2 approval (routine)	≤24 hours from request	Governance notification at 48 hours
Tier 2 approval (emergency)	≤2 hours from request	Alternate approver activated at 3 hours
Post-access review (PARP) completion	≤5 business days from access termination	Compliance alert at 7 business days; governance notification at 10
TTL expiry enforcement	Automatic at TTL endpoint	Overdue access generates ACCS compliance alert

T.6 Recall Response SLAs

Recall Action	SLA	Escalation
Recall notification issuance	≤4 hours from recall determination	Immediate governance notification if delayed
Custody holder acknowledgment	≤48 hours from notification receipt	Escalation to recall authority at 72 hours; regulatory consideration at 96 hours
Quarantine of affected units	≤24 hours from acknowledgment	Governance notification if not quarantined within 48 hours
Recall scope reconciliation (interim)	Weekly during active recall	Governance review at each interim
Recall closure	When 100% units accounted for; or governance-approved exception	Governance escalation if >90 days without closure

T.7 Governance Response SLAs

Governance Action	SLA	Escalation
Material change trigger documentation	≤24 hours from trigger detection	Auto-alert to governance body at 48 hours
Material change governance response	≤5 business days from trigger documentation	Steering Committee notification at 10 business days
Recertification cycle completion	Per cadence schedule (annual, semi-annual, quarterly per type)	Governance alert at 30 days overdue; operational restriction at 60 days overdue

Governance Action	SLA	Escalation
Liability trigger response (SEV-1)	≤2 hours from detection	Immediate regulatory liaison activation
Liability trigger response (SEV-2)	≤8 hours from detection	Governance body notification
Change Control Board review of proposed change	≤10 business days from submission	Steering Committee escalation at 20 business days

T.8 Evidence Integrity Verification SLOs

Verification Type	Cadence	Target	Escalation
Hash chain verification (custody events)	Per reconciliation cadence	100% verification pass rate	Any failure → BRK-INTEG-002; SEV-1
Content-address verification (stored artifacts)	Weekly sample (10% of active artifacts) + full scan monthly	100% verification pass rate	Any failure → BRK-INTEG-001; SEV-1
Manifest self-referential hash verification	At each manifest access and monthly full scan	100% pass rate	Any failure → BRK-INTEG-004; SEV-1
Evidence chain-of-custody completeness	Quarterly audit (sample-based)	100% of sampled artifacts have complete chain-of-custody	Gaps → RECON-008 check failure
Replication lag (between primary and replica storage)	Continuous monitoring	≤15 minutes for critical evidence; ≤1 hour for standard	Lag exceeding threshold → availability alert

T.9 Offboarding SLOs

Offboarding Activity	SLO	Escalation
Final state snapshot generation	≤5 business days from offboarding initiation	Governance notification if delayed
Final reconciliation execution	≤10 business days from snapshot completion	Governance escalation at 15 business days
Legacy transition manifest generation	≤10 business days from reconciliation completion	Governance notification if delayed
Evidence transfer to legacy system	Per offboarding plan (typically ≤15 business days)	Governance review if transfer at risk
Post-transfer verification	≤5 business days from transfer completion	Offboarding cannot close without verification
Post-offboarding monitoring initiation	Immediate upon offboarding completion	Governance alert if not initiated within 5 business days

T.10 Consolidated SLA/SLO Summary by Domain

Domain	Critical SLA	Most Impactful SLO	Governance Escalation Trigger
Evidence	Emergency: 4 hours	Standard query: 48 hours	>72 hours without

Domain	Critical SLA	Most Impactful SLO	Governance Escalation Trigger
retrieval			response
Reconciliation	Continuous for critical; daily batch for standard	No reconciliation cycle missed by >24 hours	2+ consecutive cycles missed
Break resolution	SEV-1 containment: 15 minutes	SEV-2 full resolution: 10 business days	Any SEV-1 unresolved >48 hours
Tiered access	Emergency Tier 2: 2 hours	PARP completion: 5 business days	PARP overdue >10 business days
Recall	Notification: 4 hours; acknowledgment: 48 hours	Closure: 100% units accounted	>90 days without closure
Governance	LT SEV-1 response: 2 hours	Recertification on schedule	>60 days overdue recertification
Evidence integrity	Any failure: immediate containment	100% verification pass rate	Any integrity failure (SEV-1)
Offboarding	Per plan; typically 30–60 days total	Post-transfer verification: 5 business days	Verification incomplete at offboarding close

Appendix U — Adversarial Failure Patterns, Abuse Cases, and Containment Logic for Product Authenticity, Authorization, Custody, Proof-of-Safety, and Claim Workflows

U.0 Purpose and Reader Orientation

This appendix identifies, classifies, and operationalizes adversarial failure patterns and abuse cases that the framework must detect, contain, preserve, replay, and correct. It goes beyond the reconciliation break taxonomy (Appendix C) by focusing on intentional or structurally adversarial conditions — not merely operational mismatches. Each pattern maps to detection logic, severity, containment, preservation, replay, corrective response, and governance controls.

Reader path: Operators start at U.1–U.3 for pattern recognition. Incident responders focus on U.5–U.7. Governance bodies use U.8–U.10. Examiners use U.11 for worked adversarial cases and U.12 for action routing.

U.1 Failure and Abuse Taxonomy

Failure Taxonomy Table:

Failure Class	Code	Definition	Distinguishing Feature
Operational failure	FAIL-OPS	Unintentional system error, configuration mistake, or process deviation	No intent; correctable through standard break resolution
Data integrity failure	FAIL-INTEG	Evidence artifact tampered, corrupted, or silently overwritten	May be intentional or accidental; requires forensic investigation
Adversarial injection	FAIL-ADV-INJ	False or fabricated evidence introduced into the evidence chain	Intentional; designed to deceive downstream consumers
Adversarial suppression	FAIL-ADV-SUP	Legitimate evidence withheld, deleted, or rendered inaccessible	Intentional concealment; may mask counterfeit, diversion, or unauthorized action
Authority abuse	FAIL-AUTH-AB	Legitimate credentials used outside authorized scope, time, or purpose	Actor holds valid credentials but exceeds bounds
Reviewer access abuse	FAIL-REV-AB	Tiered access used outside documented purpose, scope, or TTL	Surveillance creep, unauthorized data extraction, or scope violation
Collusion pattern	FAIL-COLLU	Multiple actors coordinating to circumvent controls	Requires multi-party detection; individual actions may appear legitimate
Replay / duplication attack	FAIL-REPLAY	Previously valid evidence or authorization reused outside its intended context	Exploits absence of freshness or nonce controls

---

U.2 Adversarial Abuse Pattern Families

Abuse Pattern Table:

Pattern ID	Pattern Name	Domain	Description	Target Control
ABP-001	Counterfeit product insertion	Product authenticity	Fabricated CPO or provenance manifest introduced to legitimize counterfeit product	PAES integrity; provenance chain verification
ABP-002	Provenance chain forgery	Provenance	Fabricated custody events inserted into provenance manifest to fill gaps or create false chain	Hash chain verification; actor credential check
ABP-003	Credential impersonation	Authorization	Forged or stolen issuer credentials used to generate authorizations	AES issuer legitimacy; revocation check freshness
ABP-004	Prescription replay	Authorization	Expired, superseded, or consumed prescription re-presented for additional dispensation	Supersession chain; quantity bound tracking; freshness check
ABP-005	Custody diversion	Custody	Products diverted from legitimate custody chain through undocumented handoffs	Custody event completeness; handoff pair matching
ABP-006	Safety evidence fabrication	Proof-of-safety	Fabricated DS or PS evidence classes created to satisfy dispensation gates	SES integrity verification; source version cross-check
ABP-007	Claim duplication	Claims	Same dispensation event claimed multiple times under different claim identifiers	CG-6 duplicate detection; dispensation-claim linkage uniqueness
ABP-008	Reviewer scope creep	Bounded review	Tier 1 or Tier 2 access used to extract data beyond approved scope or purpose	Purpose code enforcement; PARP scope verification
ABP-009	Silent evidence overwrite	Evidence integrity	Evidence artifact modified post-storage without EP Delta generation	Content-address verification; periodic hash scan
ABP-010	Collusive release bypass	Dispensation	Multiple actors collaborate to bypass dispensation precondition gates through coordinated override	Override documentation review; separation-of-duties verification

---

U.3 Detection Logic and Control Triggers

Detection Trigger Matrix:

Pattern ID	Primary Detection Method	Secondary Detection	Automated?	Trigger Event Code
ABP-001	Content-address mismatch between CPO and manufacturer registry	Cross-reference with external product identification systems	Yes	BRK-INTEG-001 or BRK-PROV-003
ABP-002	Hash chain break in provenance manifest; actor credential not in authorized registry	Temporal sequence analysis (events out of logical order)	Yes	BRK-INTEG-002 or BRK-PROV-002
ABP-003	AES revocation check returns REVOKED or credential hash mismatch	Credential usage pattern anomaly (issuing from unusual location/time)	Yes (revocation); pattern analysis semi-automated	BRK-AUTH-002 or BRK-AUTH-003
ABP-004	Quantity bound exceeded; supersession chain shows SUPERSEDED or EXPIRED	Dispensation event referencing authorization already fully consumed	Yes	BRK-AUTH-001 or quantity threshold breach
ABP-005	Custody gap (CUS_HANDOFF without matching CUS_RECEIPT); product appears at unexpected location	Aggregate quantity reconciliation: units in custody chain ≠ units released by manufacturer	Partial (gap detection automated; location anomaly requires analysis)	BRK-CUST-001 or BRK-PROV-001
ABP-006	SES evidence class references source version that does not exist or was not current at claimed timestamp	Cross-check DS output against CDSS audit log for claimed algorithm version	Partial	BRK-SAFE-001 or BRK-INTEG-001
ABP-007	Duplicate dispensation reference across multiple claim IDs	Claim-dispensation linkage uniqueness constraint violation	Yes	BRK-CLAIM-003
ABP-008	PARP scope review identifies data accessed outside approved purpose code	Access log analysis: artifacts accessed not in approved scope definition	Post-hoc (PARP review)	ACCS compliance alert
ABP-009	Periodic hash verification detects content-address mismatch for stored artifact	EP Delta chain discontinuity: artifact version changed without delta record	Yes (hash scan)	BRK-INTEG-005; liability trigger LT-07
ABP-010	Override documentation review: multiple overrides from same dispensation point in short window with same approver pair	Separation-of-duties analysis: override approver is also the dispensing actor	Post-hoc (audit)	DISP check failures; governance alert

U.4 Severity Bands and Materiality Framework

Severity and Materiality Matrix:

Pattern ID	Base Severity	Aggravating Factors (Escalate +1)	Materiality Threshold	Preservation Required
ABP-001	SEV-1 (Critical)	Multiple units; narrow therapeutic index product; distribution already commenced	Any confirmed instance	Always — PB mandatory
ABP-002	SEV-1 (Critical)	Affects chain segment already used for dispensation	Any confirmed instance	Always
ABP-003	SEV-1 (Critical)	Dispensation already completed under forged credentials; patient harm potential	Any confirmed instance	Always
ABP-004	SEV-2 (High)	Controlled substance; pattern across multiple pharmacies	≥2 instances from same authorization	Yes if SEV-1 or repeated
ABP-005	SEV-2 (High)	Cold-chain product; high-value product; pattern across multiple lots	≥1 confirmed diversion event	Yes
ABP-006	SEV-2 (High)	High-impact decision context; override based on fabricated evidence	Any confirmed fabrication	Yes
ABP-007	SEV-2 (High)	Amount exceeds institutional threshold; pattern from same claimant	≥2 duplicates from same source in 90 days	Yes if pattern detected
ABP-008	SEV-2 (High)	Sensitive data accessed (patient identity, commercial terms); repeated pattern	Any confirmed scope violation at Tier 2	Yes
ABP-009	SEV-1 (Critical)	Affects evidence supporting active dispensation or claim; deliberate tampering indicators	Any confirmed instance	Always
ABP-010	SEV-2 (High)	Controlled substance; bypassed safety gates; patient harm potential	≥3 coordinated overrides in 30 days from same point	Yes

---

U.5 Containment Logic

Containment Logic Table:

Pattern ID	Immediate Containment	Scope Determination	Hold Duration	Release Condition
ABP-001	Quarantine all units with matching CPO; block dispensation	All units from same batch/lot; trace aggregation hierarchy	Until investigation complete; governance approval for release	Counterfeit determination: destroy. Not counterfeit: release with correction EP Delta
ABP-002	Hold-only on all	Products whose	Until chain repaired or	Valid provenance

Pattern ID	Immediate Containment	Scope Determination	Hold Duration	Release Condition
	products in affected chain segment	provenance manifest includes the forged event(s)	products re-verified through independent evidence	established through alternative evidence; governance approval
ABP-003	Hold all pending dispensation under affected authorizations; flag completed dispensation for review	All authorizations issued by the impersonated credential	Until credential fraud confirmed or denied	Fraud denied: release. Fraud confirmed: all authorizations revoked; patient notification
ABP-004	Block further dispensation under the replayed authorization	Single authorization + all dispensation points that processed it	Until quantity reconciliation confirms actual dispensation count	Quantity reconciled; excess dispensation investigated
ABP-005	Hold-only on all products last known in the diverted segment	Products in custody gap segment; potentially broader if quantity discrepancy detected	Until products located and verified or loss confirmed	Products verified at known location; or loss documented with governance approval
ABP-006	Hold on dispensation events relying on fabricated evidence; re-assess safety	Dispensation events where SES references the fabricated artifact	Until legitimate safety evidence regenerated	Fresh SES generated from verified source; dispensation re-assessed
ABP-007	Hold both claims; block payout on duplicates	All claims referencing the same dispensation event	Until duplicate confirmed and one claim denied	Investigation determines legitimate claim; duplicate denied
ABP-008	Terminate active access session; revoke access grant	Single access event + review of other access by same reviewer in rolling 90 days	Access terminated immediately; investigation period per governance SLA	PARP completed; scope violation assessed; disciplinary or corrective action per institutional policy
ABP-009	Hold all dependent operational states; recover valid version from backup	All states and downstream actions referencing the overwritten artifact	Until valid version restored and dependent states re-verified	Valid version restored; integrity confirmed; dependent states re-assessed
ABP-010	Suspend override authority at affected dispensation point; hold pending dispensation	All dispensation events approved through the suspected collusive pattern	Until separation-of-duties audit completed	Audit confirms no collusion: restore authority. Collusion confirmed: institutional corrective action

U.6 Preservation and Replay Requirements

Preservation Requirement Matrix:

Pattern ID	PB Trigger	Minimum PB Contents	Retention
ABP-001	Confirmed or suspected counterfeit	CPO evidence; provenance manifest; PAES; manufacturer communication; quarantine records; investigation report	Indefinite
ABP-002	Confirmed hash chain forgery	Original and forged provenance events; hash verification failure evidence; forensic investigation records	Indefinite
ABP-003	Confirmed or suspected credential fraud	Forged credential evidence; legitimate credential comparison; all authorizations issued under forged credential; dispensation records	Indefinite
ABP-004	Confirmed prescription replay	Original authorization with lifecycle; all dispensation events; quantity tracking records; supersession chain	7+ years
ABP-005	Confirmed diversion	Custody event chain with gap; quantity reconciliation; investigation records; any recovery evidence	Indefinite
ABP-006	Confirmed safety evidence fabrication	Fabricated artifact; source system audit log; SES records; affected dispensation events; clinical re-assessment records	Indefinite
ABP-007–ABP-010	Per severity assessment	Pattern-specific evidence per containment scope	Per institutional retention policy; minimum 7 years

Replay Requirement Matrix:

Pattern ID	Replay Scope	Replay Purpose	Minimum Replay Capability
ABP-001	Full provenance chain for affected batch/lot	Determine where counterfeit entered the chain	Event-by-event provenance replay with integrity verification at each link
ABP-002	Provenance manifest event sequence	Identify forged events and determine scope of affected products	Hash-verified event replay with forensic comparison against backup copies
ABP-003	All authorizations and dispensation events under affected credential	Identify all potentially unauthorized actions	Authorization lifecycle replay + dispensation gate result replay
ABP-004	Authorization lifecycle + all dispensation events	Determine total actual dispensation vs. authorized quantity	Full quantity tracking replay across all dispensation points
ABP-005	Custody event chain for affected products	Determine where diversion occurred and scope of loss	Custody event replay with gap identification and location analysis
ABP-006	SES at dispensation time + CDSS audit log	Determine whether fabricated evidence	Decision state replay (Section 7.3) with source version cross-

Pattern ID	Replay Scope	Replay Purpose	Minimum Replay Capability
		influenced clinical decisions	verification

U.7 Corrective Action and EP Delta Discipline

Correction / EP Delta Matrix:

Pattern ID	Corrective Action	EP Delta Required	Non-Destructive Preservation
ABP-001	Counterfeit confirmed: revoke PAES; quarantine/destroy product; notify downstream	Yes — PAES state → AUTH_FAILED; provenance → PROV_BROKEN	Original PAES and provenance preserved in PB
ABP-002	Remove forged events; reconstruct chain from verified evidence; generate corrected provenance manifest	Yes — provenance manifest superseded by corrected version	Forged events preserved in PB; corrected manifest becomes current-reference
ABP-003	Revoke all authorizations under forged credential; generate revocation EP Deltas per authorization	Yes — each affected authorization → RX_REVOKED	Original authorizations preserved; revocation records document fraud basis
ABP-004	Reconcile actual dispensation quantity; block further dispensation; generate quantity correction	Yes — authorization quantity tracking corrected; excess dispensation documented	Replay evidence preserved; excess dispensation flagged for clinical follow-up
ABP-005	Document confirmed diversion; adjust custody chain; generate loss record	Yes — custody state → CUST_COMPROMISED for affected segment	Original custody evidence preserved; diversion documented
ABP-006	Invalidate fabricated evidence; regenerate safety evidence from verified sources; re-assess affected dispensation	Yes — SES superseded with fresh evidence from verified source	Fabricated artifact preserved in PB; fresh SES becomes current-reference
ABP-009	Restore valid version from backup; re-verify dependent states	Yes — EP Delta documenting restoration; integrity incident record	Overwritten version and restored version both preserved

U.8 Override, Exception, and Governance Controls

Override Governance Matrix:

Override Type	Authority Required	Documentation	Governance Review	Recurrence Limit
Dispensation gate override (single gate, non-safety)	Qualified pharmacist + supervisor	DS-05 equivalent justification; accountability insert	Quarterly review of override volume	≥5 overrides/month at same point triggers governance review
Dispensation gate override (safety gate)	Senior clinician + pharmacy director	Full clinical justification; Exceptional review posture	Each instance reviewed within 5 business days	≥3 safety gate overrides/quarter triggers institutional review
Hold release without full resolution	Governance body approval	Resolution-in-progress documentation; risk acceptance record	Governance approval documented	No recurrence limit; each case individually approved
Tier 2 access extension beyond initial TTL	Dual-control re-approval	Updated justification; renewed scope definition	Each extension reviewed in PARP	≥3 extensions for same investigation triggers governance review
Correction without standard approval chain (emergency)	Emergency authority per institutional policy	Post-hoc full documentation within 24 hours	Mandatory governance review within 5 business days	Each emergency correction individually reviewed

---

U.9 Reviewer / Examiner Access Abuse and Bounded Verification Controls

Reviewer Access Abuse Matrix:

Abuse Type	Detection Method	Containment	Governance Response
Scope violation — data accessed outside approved purpose code	PARP scope verification; access log analysis	Terminate access; revoke grant	Institutional disciplinary process; access restriction
TTL violation — access continues beyond expiry	Automated TTL enforcement (should prevent); manual detection if enforcement fails	Force session termination; log enforcement failure as system incident	System control remediation; access governance review
Frequency anomaly — reviewer accesses same subject repeatedly without documented justification	Access frequency monitoring; threshold alerts	Flag for governance review; no automatic termination	Governance assessment of access pattern; potential restriction
Data exfiltration indicator — bulk download or export beyond review purpose	Export volume monitoring; anomaly detection	Terminate access; hold exported data if possible; preserve access logs	Incident investigation; institutional and potentially regulatory response

Abuse Type	Detection Method	Containment	Governance Response
Collusive access — reviewer and operator coordinate to bypass minimization	Post-hoc pattern analysis comparing operator actions and reviewer access timing	Suspend both parties' access; investigation	Governance investigation; dual accountability

U.10 Residual Risk Register

Residual Risk Register:

Risk ID	Residual Risk	Mitigating Controls	Residual Severity	Monitoring
RR-001	Counterfeit products with perfect provenance forgery (if hash algorithm compromised)	Crypto-agility baseline (Baseline B); periodic algorithm assessment; multi-source corroboration	Low (with current algorithms)	Algorithm lifecycle monitoring per Baseline B
RR-002	Insider with legitimate credentials and system access fabricating evidence	Separation of duties; multi-party controls; audit trail review; behavioral anomaly detection	Moderate	Periodic audit of evidence generation patterns
RR-003	Coordinated multi-party collusion exceeding governance quorum requirements	No-master-key posture; distributed governance; rotation of governance roles	Low	Governance composition review at recertification
RR-004	Reviewer access abuse not detected within TTL window	TTL enforcement; PARP review; access frequency monitoring	Moderate	PARP completion rate monitoring; access pattern analysis
RR-005	Cross-border evidence portability gaps exploited for regulatory arbitrage	Equivalence assessment discipline; cross-domain reconciliation; jurisdiction-bounded review	Moderate	Cross-border evidence quality assessment at portability events

U.11 Worked Adversarial Mini-Scenarios

Worked Scenario Summary Table:

Scenario	Pattern	Detection	Containment	Resolution	Evidence Preserved
Distributor substitutes lower-cost product with matching labels into legitimate custody chain	ABP-001 + ABP-005	CPO hash mismatch at pharmacy receipt verification	Quarantine all units from shipment; hold on distributor's custody chain	Investigation confirms substitution; product destroyed; distributor suspended	PB with provenance, custody, and substitution evidence
Expired prescription photo-copied and re-presented at multiple pharmacies	ABP-004	Quantity bound exceeded across pharmacies; authorization state	Block all dispensation under the authorization;	Quantity reconciled; excess dispensation	Authorization lifecycle; dispensation records across

Scenario	Pattern	Detection	Containment	Resolution	Evidence Preserved
		= RX_EXPIRED	recall evidence from pharmacies	documented; prescriber and pharmacies notified	pharmacies; quantity tracking
Hospital system administrator modifies stored safety evidence to suppress contraindication alert history	ABP-009	Periodic hash verification detects content-address mismatch on SES artifact	Hold all dependent dispensation; recover valid SES from backup	Valid SES restored; investigation of administrator actions; institutional corrective action	Original, tampered, and restored versions all preserved; access logs
Examiner uses Tier 2 access for broad patient data extraction beyond investigation scope	ABP-008	PARP review identifies artifacts accessed outside approved scope definition	Access terminated; exported data quarantined	Governance investigation; access restriction; potential regulatory reporting	Access logs; PARP; scope violation documentation

---

U.12 Reader Action Map

Reader Action Map:

Reader Profile	Start Here	Key Tables	Primary Actions
Incident responder	U.3 (Detection), U.5 (Containment)	Detection Trigger Matrix, Containment Logic Table	Identify pattern; apply containment; initiate preservation
Investigator	U.6 (Preservation/Replay), U.7 (Correction)	Preservation/Replay matrices; Correction/EP Delta matrix	Gather evidence; replay events; determine corrective action
Governance body	U.8 (Override), U.10 (Residual Risk)	Override Governance Matrix; Residual Risk Register	Review overrides; assess residual risk; approve corrective actions
Examiner / auditor	U.11 (Worked Scenarios), U.9 (Access Abuse)	Worked Scenario Table; Reviewer Access Abuse Matrix	Verify detection controls; assess containment adequacy; review access compliance
Operator (pharmacy, distributor, manufacturer)	U.1 (Taxonomy), U.2 (Patterns)	Failure Taxonomy; Abuse Pattern Table	Recognize patterns; implement detection; prepare for containment

---

Appendix V — Canonical State, Version Supersession, and Authority-to-Release / Authority-to-Dispense Controls

V.0 Purpose and Reader Orientation

This appendix defines how canonical state (the single authoritative current-reference version), supersession chains, authority-to-release, authority-to-dispense, authority-to-correct, rollback posture, and downstream propagation operate across all framework domains. It deepens the version lineage templates (Appendix L) with operational decision logic.

V.1 Canonical State Taxonomy

Canonical State Taxonomy Table:

Domain	Canonical Object	Canonical Determination Method	Authoritative Source
Product identity	CPO (current version)	Most recent non-revoked version in version lineage	Manufacturer or authoritative product registry
Provenance	Provenance manifest (current version)	Most recent manifest incorporating all verified custody events	Aggregated from custody event producers; assembled by provenance coordinator
Authorization	Prescription / authorization (current in supersession chain)	Most recent non-revoked, non-superseded version in supersession chain	Issuing prescriber or governance body
Issuer legitimacy	AES (current verification)	Most recent verification within freshness window with revocation check CLEAR	Credentialing body via verification process
Custody	CES (current chain endpoint)	Most recent custody event in hash-chained sequence	Current custodian's custody event log
Safety evidence	SES (current set)	Most recent set where all required evidence classes are current relative to source data versions	Clinical systems; formulary; decision-support systems
Dispensation	DEP-H (immutable once generated)	No supersession; dispensation events are terminal — corrections create new records, not versions	Dispensing entity
Claim	CLM-EP (current lifecycle state)	Most recent lifecycle event in claim chain	Benefit administrator

---

V.2 Authority-to-Release / Authority-to-Dispense Model

Authority-to-Release / Authority-to-Dispense Matrix:

Action	Required Authority	Evidence of Authority	Freshness Requirement	Failure Response
Release product from quarantine	Quality function + governance approval	Resolution evidence; quality assessment; governance approval record	Event-driven (at release decision)	Release blocked if approval incomplete
Release hold-only containment	Authority that imposed hold, or governance body	Resolution evidence; approval chain per Appendix F hold-set template	Event-driven	Hold continues until authorized release
Dispense product to recipient	Dispensing entity with valid dispensation credential; all G1–G7 gates passed	DEP-H with complete gate results; dispensing entity AES	Gates verified at dispensation time	Dispensation blocked at failing gate
Authorize prescription	Licensed prescriber with ISSU_CONFIRMED; scope covers product	AES with all bound categories verified	Issuer credential within freshness window	Authorization not valid; cannot support dispensation
Correct evidence artifact	Originating entity + supervisor (routine); governance body (material)	Correction EP Delta with approval chain	At correction time	Correction blocked without required approvals
Revoke authorization	Issuing authority, credentialing body, or governance body	Revocation record per Appendix L template	Immediate effect	Downstream propagation initiated
Approve claim for payout	Benefit administrator; all CG gates passed	CLM-EP with complete gate results and temporal assessment	At adjudication time	Claim pended or denied

V.3 Canonical Determination Logic

Canonical Determination Logic Table:

Condition	Determination Rule	Example
Single version exists, not revoked	That version is canonical	Newly issued prescription — only version
Multiple versions; clear supersession chain	Latest non-revoked version in chain is canonical	Prescription renewed twice — v3 is canonical
Latest version revoked; prior versions exist	Canonical = null; re-authorization required	Prescription v3 revoked; v1 and v2 are SUPERSEDED, not eligible as fallback

Condition	Determination Rule	Example
Parallel versions (no supersession relationship)	Conflict detected; hold-only containment on all; governance resolution required	Two prescriptions from different prescribers for same product/patient without supersession linkage
Version under correction (EP Delta pending)	Prior version remains canonical until correction finalized and approved	CPO v2 correction in progress; v1 still governs until v2 approved
All versions expired	Canonical = null (EXPIRED); new authorization required	Prescription with all versions past validity_end

V.4 Version Supersession Discipline

Supersession Chain Matrix:

Rule	Requirement	Violation Response
Ordered chain	Each version links to its predecessor through content-addressed reference	Chain break → BRK-INTEG; hold-only on affected states
Single current	Exactly one version with status CURRENT at any time (or zero if revoked/expired)	Multiple CURRENT → conflict resolution per V.7
Non-destructive	Superseded versions preserved; accessible for replay	Destruction of superseded version → governance violation (LT-07)
EP Delta at each transition	Every version change produces EP Delta	Missing EP Delta → BRK-INTEG-005; correction required
Temporal consistency	Each version effective_from ≥ predecessor effective_until	Temporal overlap → investigation of backdating
Downstream propagation	Actions bound to superseded version generate reconciliation break	Dispensation referencing superseded authorization → BRK-AUTH break

V.5 Product, Authorization, Custody, and Canonical-State Relationships

State Relationship Table:

Upstream Canonical State	Downstream Dependent States	Binding Requirement
CPO (canonical product identity)	PAES, provenance manifest, CES events, SES product-level classes	All downstream artifacts reference CPO content_address; CPO change propagates as material change trigger
AES (canonical issuer legitimacy)	Prescription validity, dispensation authorization, delegation chain	Dispensation gates reference current AES; AES revocation propagates to dependent authorizations
Prescription (canonical authorization)	Dispensation events, claim linkage, refill tracking	Dispensation binds to current-reference prescription; superseded prescription cannot support new dispensation
SES (canonical safety evidence)	Dispensation safety gate, decision state records	Dispensation gate G5 references current SES; superseded SES cannot satisfy gate without refresh
CES (canonical	Dispensation custody gate,	Dispensation gate G4 references current CES

Upstream Canonical State	Downstream Dependent States	Binding Requirement
custody chain)	provenance alignment	endpoint; custody break holds dispensation

V.6 Downstream Binding to Canonical State

Downstream Binding Matrix:

Downstream Action	Must Bind To	Verification At	Stale Binding Response
Dispensation	Current CPO, current AES, current CES endpoint, current SES	Each dispensation event (gates G1–G7)	BRK break per domain; dispensation blocked
Claim submission	DEP-H (immutable) → which references PAES, AES, CES, SES at dispensation time	Claim validation (gates CG-1–CG-6); temporal assessment	Gate failure; claim pended
Refill	Current prescription version in supersession chain; current AES	Each refill event	Stale binding generates BRK-AUTH; refill blocked
Recall scope	Canonical CPO batch/lot reference	Recall initiation	Incorrect CPO reference → scope error; correction per recall scope EP Delta
Offboarding snapshot	All canonical states at snapshot time	Final state snapshot generation	Snapshot references non-current version → reconciliation break in final reconciliation

V.7 Conflict and Parallel-State Resolution

Conflict Resolution Matrix:

Conflict Type	Detection	Default Response	Resolution Authority	Evidence
Parallel prescriptions (no supersession)	Reconciliation detects multiple RX_VALID for same scope	Hold-only on all affected prescriptions	Institutional governance (Pharmacy and Therapeutics equivalent)	Determination record specifying which becomes canonical; others SUPERSEDED
Conflicting custody claims	Two entities claim current custody of same product unit	Hold-only on product; no transfer or dispensation	Investigation with both parties; governance determination	Custody evidence from both parties; determination with supporting evidence
Divergent safety assessments	Two evidence classes produce contradictory safety conclusions	SAFE_DISPUTED state; hold on dispensation	Clinical review authority	Clinical determination record; resolution EP Delta

Conflict Type	Detection	Default Response	Resolution Authority	Evidence
Version lineage fork (two corrections applied independently)	Hash chain verification shows branch point	Hold-only; both branches preserved	Governance body determines authoritative branch	Investigation of fork cause; single branch designated canonical; other archived

V.8 Evidence, Manifest, and Preservation Requirements for State Changes

State-Change Artifact Requirement Matrix:

State Change Type	Required Artifacts	Content-Addressed	Linked To	Retention
Version creation (genesis)	Initial record + manifest entry	Yes	Lineage record (Appendix L)	Per domain retention
Supersession	EP Delta (prior → new); supersession chain update	Yes	Preceding version; succeeding version	Both versions retained
Correction	Correction EP Delta; approval chain; prior/new content addresses	Yes	Version lineage; break record (if break-triggered)	Both versions retained
Revocation	Revocation record (Appendix L); downstream impact assessment	Yes	All dependent downstream states	Indefinite
Reclassification	Reclassification EP Delta; governance approval	Yes	Prior classification; new classification	Both retained
Expiry	Expiry detection record	Yes	Version lineage; temporal bound fields	Per domain retention
Hold entry / release	Hold-set record (Appendix F)	Yes	Triggering condition; resolution evidence	Per domain retention

V.9 Correction, Reclassification, Revocation, and Replay

Correction / Revocation / Reclassification Matrix:

Action	Authority	EP Delta Required	Downstream Propagation	Replay Capability
Factual correction	Originating entity + supervisor	Yes	Identify and re-verify all downstream actions referencing pre-correction version	Pre- and post-correction states both replayable

Action	Authority	EP Delta Required	Downstream Propagation	Replay Capability
Reclassification (e.g., product category change)	Governance body	Yes	Material change trigger; downstream re-assessment required	Historical classification preserved; reclassification context replayable
Revocation (authorization)	Issuing authority or governance	Yes	All dependent dispensation and claims assessed; holds applied to pending actions	Full authorization lifecycle replayable; revocation context preserved
Revocation (credential)	Credentialing body	Yes	All authorizations under credential assessed; BRK-AUTH-004 workflow	Credential lifecycle + all dependent authorization lifecycles replayable
Rollback (system-level)	Governance body + technical authority	Yes (documenting rollback)	All states restored to pre-change condition; post-rollback verification	Pre-change, post-change, and rollback states all preserved

V.10 Governance, Override, and Exception Controls

Override and Exception Governance Matrix:

Override / Exception	Required Authorization	Documentation	Review Cadence
Accept non-canonical state for dispensation (emergency)	Senior clinician + governance	Emergency justification; Exceptional review posture	Each instance within 5 business days
Override conflict resolution determination	Governance body (Steering Committee equivalent)	Documented rationale; dissenting positions recorded	At determination time
Extend hold beyond maximum duration	Governance body	Updated justification; continued necessity assessment	At each extension
Accept correction without full investigation (low-severity)	Operational management (dual approval)	Abbreviated investigation summary	Quarterly aggregate review

V.11 Reviewer / Examiner Determination Paths

Reviewer / Examiner Determination Matrix:

Examiner Question	Evidence Path	Tier
"What is the canonical state of product X right now?"	CPO version lineage → current-reference hash → PAES	Tier 1
"Was this dispensation bound to the	DEP-H → authorization reference → supersession	Tier 1

Examiner Question	Evidence Path	Tier
correct canonical authorization?"	chain → current-reference at dispensation time	
"Were there any parallel-state conflicts for this product?"	Reconciliation break records → BRK-AUTH-006 or conflict resolution records	Tier 1
"Show the full version lineage for this prescription"	Version lineage record → EP Delta chain → all versions	Tier 1
"Was the authority-to-dispense properly established?"	DEP-H gate results → AES → issuer credential → scope verification	Tier 1

V.12 Offboarding and Legacy State Portability

Offboarding State Portability Matrix:

State Element	Portable to Legacy	Data Loss Risk	Mitigation
Current-reference state values	Yes — exportable as structured data	Low	Standard field mapping
Supersession chain (full history)	Partial — legacy may not support chain structure	Moderate	Archive full chain in framework storage; export current-reference only to legacy; document chain availability
EP Delta chain	Partial — legacy may not support delta chaining	Moderate	Archive deltas; export summary corrections to legacy
Content addresses / hash linkage	Rarely — legacy systems typically lack content addressing	High for integrity verification	Archive content-addressed originals; export plain-text equivalents with integrity attestation
Revocation records	Yes — exportable as event records	Low	Standard event mapping

---

V.13 Worked Mini-Scenarios

Worked Scenario Summary Table:

Scenario	Domain	Canonical Issue	Resolution
Two pharmacies hold different prescription versions for same patient/product; neither shows supersession linkage	Authorization	Parallel-state conflict	Governance resolution: prescriber confirms intended current prescription; other SUPERSEDED; EP Delta chain repaired
Hospital formulary change supersedes safety evidence for 200 active prescriptions; 15 dispensation events pending	Safety / dispensation	Mass supersession triggering cascade of gate failures	Batch SES refresh against new formulary; 12 of 15 dispensation events clear after refresh; 3 require prescriber re-assessment
Product CPO corrected (wrong batch/lot reference); 50 downstream PAES	Product identity	Correction propagation across large artifact	Correction EP Delta for CPO; batch re-linkage of 50 PAES artifacts; reconciliation confirms

Scenario	Domain	Canonical Issue	Resolution
artifacts reference old CPO		population	all 50 updated

V.14 Reader Action Map

Reader Profile	Start Here	Key Tables	Primary Actions
Dispensation system implementer	V.2, V.6	Authority Matrix; Downstream Binding Matrix	Configure gate logic to reference canonical states
Governance body	V.7, V.10	Conflict Resolution Matrix; Override Matrix	Adjudicate conflicts; approve exceptions
Examiner	V.11, V.3	Determination Matrix; Canonical Logic Table	Verify canonical state determination; audit version lineage
Offboarding coordinator	V.12	Portability Matrix	Plan legacy transition for version history and canonical state

Appendix W — Claim, Reimbursement, Settlement, and Dispute-Resilient Payout Controls

W.0 Purpose and Reader Orientation

This appendix deepens Section 12 and Appendix P with a complete operational model for financially consequential healthcare workflows. It is conditional — included only where claim, reimbursement, settlement, or payout workflows are in scope. It does not dominate the framework; every financial control links back to product authenticity, authorization, custody, and proof-of-safety sufficiency.

W.1 Revenue / Claim Event Taxonomy

Claim / Event Taxonomy Table:

Event Category	Event Codes	Description	Evidence Linkage
Dispensation-triggered claim	CLM_SUBMITTED through CLM_PAID (per Section 12.1)	Standard reimbursement claim for a dispensation event	DEP-H → PAES, AES, CES, SES
Service-triggered claim	SVC_SUBMITTED, SVC_VALIDATED, SVC_ADJUDICATED, SVC_APPROVED, SVC_PAID	Claim for clinical service (administration, counseling, assessment) linked to product event	Service record → authorization → product reference (if applicable)
Adjustment event	CLM_ADJUSTED, CLM_REVERSED (per Section 12.6)	Post-payment correction linked to upstream evidence change	Adjustment linkage template (Appendix P, P.3)
Dispute event	DSP_INITIATED, DSP_EVIDENCE_SUBMITTED, DSP_DETERMINED, DSP_CLOSED	Claim disputed by any party; evidence-based resolution	Dispute record → original claim → all linked evidence
Recovery event	REC_INITIATED, REC_IN_PROGRESS, REC_COMPLETED, REC_WRITTEN_OFF	Recovery of overpayment or fraudulent payment	Recovery record → adjustment → original claim

---

W.2 Eligibility and Contribution / Entitlement Logic

Eligibility and Contribution Matrix:

Eligibility Dimension	Verification Source	Verification Timing	Failure Response
Beneficiary coverage active	Benefit plan enrollment records	At claim submission (CG validation)	Claim denied: coverage inactive

Eligibility Dimension	Verification Source	Verification Timing	Failure Response
Product covered under plan	Formulary / benefit schedule	At claim submission	Claim denied or pended for exception review
Authorization valid at dispensation time	AES temporal assessment	At claim validation (CG-2)	Claim pended or denied per temporal assessment
Provider/pharmacy authorized for plan	Provider credentialing records	At claim submission	Claim denied: provider not credentialed for plan
Quantity within benefit limits	Benefit accumulation tracking	At claim submission	Claim denied or pended for quantity exception

W.3 Eligibility Gates for Calculation and Payout

Eligibility Gate Matrix:

Gate	Verification	Source	Failure
EG-1: Coverage verification	Beneficiary enrolled and coverage active at dispensation date	Enrollment records	Claim denied
EG-2: Product formulary status	Product on approved formulary (or exception approved) at dispensation date	Formulary records (version at dispensation)	Claim pended for exception review
EG-3: Authorization evidence linkage	All CG gates (CG-1 through CG-6 from Section 12.2) passed	CLM-EP gate results	Claim pended or denied per CG failure type
EG-4: Provider credentialing	Dispensing entity credentialed with benefit plan	Provider records	Claim denied
EG-5: Benefit accumulation	Dispensation within benefit period limits (quantity, cost, visit count)	Accumulation tracking	Claim denied or pended
EG-6: Pricing verification	Claimed amount consistent with contracted pricing	Pricing schedules	Claim adjusted to contracted amount

W.4 Claim / Reimbursement Waterfall Model

Claim / Reimbursement Waterfall Table:

Step	Action	Input	Output	Evidence
1. Submission	Claim submitted by provider/pharmacy	Dispensation reference, product reference, authorization reference, amount	CLM_SUBMITTED event	Claim record with all linkage references
2. Validation	CG and EG gates evaluated	Claim record + upstream evidence sets	CLM_VALIDATED (if all pass) or CLM_PENDED	Gate results record
3. Pricing	Amount calculated per contracted	Contracted pricing schedule + dispensation	Priced amount (may differ from submitted amount)	Pricing calculation record

Step	Action	Input	Output	Evidence
	pricing	parameters		
4. Adjudication	Determination issued (approve, deny, pend)	Validated and priced claim + all gate results	CLM_ADJUDICATED	Adjudication record with determination and reason
5. Approval	Approved for payout	Adjudication = approved	CLM_APPROVED	Approval record with evidence sufficiency confirmation
6. Payout	Payment executed	Approval + payment instruction	CLM_PAID	Settlement confirmation
7. Reconciliation	Claim evidence reconciled periodically	Claim records + upstream evidence	Alignment or break detection	Reconciliation report

W.5 Usage, Event, and Calculation Artifacts

Usage / Event and Calculation Artifact Matrix:

Artifact	Content	Content-Addressed	Linked To	Retention
Claim submission record	All claim fields, linkage references, submission timestamp	Yes	DEP-H; AES; PAES	7+ years
Gate result record	CG-1 through CG-6 and EG-1 through EG-6 results	Yes	Claim record; upstream evidence manifests	7+ years
Pricing calculation record	Submitted amount, contracted rate, calculated amount, adjustment reason (if any)	Yes	Pricing schedule version; claim record	7+ years
Adjudication record	Determination, reason code, reviewed evidence references, adjudicator identifier	Yes	Claim record; gate results	7+ years
Settlement confirmation	Payment reference, amount, execution timestamp, settlement status	Yes	Approval record; payment system	7+ years

W.6 Settlement Confirmation and Payout Linkage

Settlement Confirmation and Payout Linkage Matrix:

Settlement Element	Verification	Evidence	Failure Response
Payout amount matches approved	Amount comparison: CLM_APPROVED.amount = CLM_PAID.amount	Settlement confirmation record	BRK-CLAIM-005 if mismatch; adjustment initiated

Settlement Element	Verification	Evidence	Failure Response
amount			
Payee matches approved payee	Payee identifier comparison	Payee verification record	Payout blocked; investigation
Settlement timing within SLA	Timestamp comparison: CLM_PAID.timestamp - CLM_APPROVED.timestamp ≤ SLA	Timing record	SLA breach logged; governance notification
No duplicate payout	Uniqueness check: single CLM_PAID per CLM_APPROVED	Duplicate detection query	BRK-CLAIM-004; immediate investigation
Evidence chain intact at payout time	Spot-check: upstream evidence still valid (no post-approval revocation)	Re-verification record	Payout held if post-approval evidence change detected

W.7 Break Taxonomy for Claim and Payout Workflows

Financial Break Taxonomy Table:

Break Code	Name	Severity	Detection	Response
BRK-FIN-001	Claim without valid dispensation evidence	SEV-2	CG-1 gate failure	Claim pended
BRK-FIN-002	Authorization invalid at dispensation time (pre-dispensation revocation)	SEV-1	CG-2 temporal assessment	Claim denied; dispensation investigation
BRK-FIN-003	Duplicate claim for same dispensation	SEV-2	CG-6 uniqueness check	Both claims held; investigation
BRK-FIN-004	Payout without approved claim	SEV-1	Reconciliation: payment without CLM_APPROVED	Immediate investigation; recovery
BRK-FIN-005	Payout amount mismatch	SEV-3 (rounding) to SEV-2 (material)	Amount comparison	Adjustment
BRK-FIN-006	Post-payment upstream evidence change	SEV-2	Reconciliation detects revocation/recall post-CLM_PAID	Adjustment or reversal assessment
BRK-FIN-007	Claim aging beyond adjudication SLA	SEV-3	Aging monitoring	Governance notification; expedited adjudication

W.8 Hold-Only Containment and Dispute-Resilient Controls

Hold-Only Containment Matrix:

Hold Trigger	Scope	Duration	Release Condition
Evidence gate failure (CG or EG)	Individual claim	Until evidence gap resolved	Evidence refreshed; gate re-evaluated and passes
Upstream evidence revocation post-approval	Claim + payout	Until impact assessment complete	Assessment determines: no impact (release) or adjustment/reversal required
Dispute initiated	Claimed amount	Until determination issued	Dispute resolved; determination executed
Duplicate detection	Both claims	Until investigation determines legitimate claim	One claim confirmed; duplicate denied
Fraud investigation	All claims from suspected source	Per investigation timeline	Investigation concluded; appropriate action taken

W.9 Adjustment, Reversal, Rebinding, and EP Delta Discipline

Adjustment / Reversal / Rebinding Matrix:

Action	Trigger	Authority	EP Delta	Recovery
Pricing adjustment	Pricing error detected post-payment	Benefit administrator (dual approval for material amounts)	Yes — CLM_ADJUSTED with amount delta	Overpayment: recovery initiated; underpayment: supplemental payment
Authorization-based reversal	Authorization revoked pre-dispensation discovered post-payment	Benefit administrator + governance	Yes — CLM_REVERSED with revocation reference	Full recovery initiated
Recall-based adjustment	Product recalled post-dispensation and post-payment	Benefit administrator	Yes — CLM_ADJUSTED with recall reference	Institutional determination: full/partial/no recovery
Evidence correction rebinding	Upstream evidence corrected (not invalidated)	Benefit administrator	Yes — claim evidence chain rebound to corrected version	No financial adjustment if correction does not change claim validity
Fraud determination reversal	Fraud investigation confirms fraudulent claim	Benefit administrator + governance + regulatory liaison	Yes — CLM_REVERSED with fraud reference	Full recovery; regulatory referral

W.10 Governance, Override, and Accountability for Payout Decisions

Governance and Accountability Matrix:

Decision	Authority	Accountability Insert Required	Review
Approve claim for payout	Benefit administrator adjudication function	Yes (standard)	Quarterly sample audit
Override gate failure for claim approval	Senior adjudicator + supervisor	Yes (enhanced — full justification)	Each override reviewed within 5 business days
Approve adjustment / reversal	Benefit administrator (dual approval)	Yes	Monthly aggregate review
Approve write-off of unrecoverable amount	Governance body	Yes (with financial impact assessment)	Each write-off individually approved
Approve payout hold release	Adjudication authority	Yes	Standard review cadence

W.11 Reviewer / Examiner Verification Paths

Reviewer / Examiner Verification Matrix:

Examiner Question	Evidence Path	Tier
"Were all claim gates properly evaluated?"	CLM-EP → gate results → upstream evidence references	Tier 1
"Was the temporal assessment correctly applied?"	CLM-EP → temporal assessment record → AES timeline	Tier 1
"Show post-payment adjustments and their triggers"	Adjustment records → upstream trigger references	Tier 1
"Are there unresolved financial breaks?"	Open breaks register (claims)	Tier 0 (aggregate); Tier 1 (individual)
"What is the recovery status for reversed claims?"	Recovery tracking records	Tier 1

W.12 Residual Balances, Unmatched Amounts, and Exception Queues

Residual Balance and Exception Queue Matrix:

Exception Type	Detection	Aging Threshold	Escalation	Disposition
Claim validated but not adjudicated	Aging monitor	>10 business days	Governance notification	Expedited adjudication
Approved but not paid	Aging monitor	>5 business days	Payment system investigation	Resolve payment issue or cancel
Recovery initiated but not completed	Aging monitor	>90 days	Governance review	Continue recovery or approve write-off
Unmatched payment (payment without claim)	Reconciliation	Any occurrence	Immediate investigation	Identify claim or recover payment
Disputed amount in hold	Dispute aging	>30 days	Governance review	Expedite determination

W.13 Offboarding and Financial-State Portability

Offboarding Financial-State Portability Matrix:

Financial Element	Portable	Legacy Requirement	Data Loss Risk
Claim lifecycle records	Yes	Claims database or archive	Low
Gate results and temporal assessments	Partial	May not support temporal assessment logic	Moderate — archive originals
Adjustment/reversal chain	Yes — as event records	Claims adjustment history	Low
Open breaks register	Yes — as structured data	Exception tracking system	Low
Evidence linkage (content-addressed)	Partial	Typically lacks content addressing	Moderate — archive with integrity attestation
Recovery tracking	Yes	Accounts receivable or recovery system	Low

---

W.14 Worked Mini-Scenarios

Worked Scenario Summary Table:

Scenario	Trigger	Key Control	Outcome
Claim submitted for recalled product; recall occurred between dispensation and claim	CG-5 detects active recall at submission	Claim pended; investigation determines product was not from recalled batch	Claim released; pended batch/lot assessment documented
Post-payment discovery: prescriber credential revoked 2 days before dispensation	BRK-FIN-002 via reconciliation	CLM_REVERSED; full recovery initiated; patient safety assessment	Recovery completed; patient care continuity confirmed
Duplicate claim from two pharmacies for same dispensation (patient obtained two fills inappropriately)	CG-6 detects duplicate dispensation reference	Both claims held; investigation reveals quantity bound exceeded	One claim approved (legitimate fill); second denied; prescription quantity tracking corrected

---

W.15 Reader Action Map

Reader Profile	Start Here	Key Tables	Primary Actions
Benefit administrator	W.3–W.4	Gate Matrix; Waterfall Table	Configure eligibility gates; implement adjudication workflow
Claims auditor	W.7, W.11	Financial Break Taxonomy; Verification Matrix	Audit gate compliance; verify temporal assessments
Governance	W.10, W.12	Accountability Matrix; Exception Queue Matrix	Approve overrides; review aging exceptions
Offboarding	W.13	Financial Portability Matrix	Plan claim data transition

Reader Profile	Start Here	Key Tables	Primary Actions
coordinator			

Appendix X — Bounded Reviewer/Examiner Verification Outputs, Minimal Disclosure Profiles, and Query-Safe Evidence Views

X.0 Purpose and Reader Orientation

This appendix operationalizes bounded verification — the discipline ensuring reviewers receive exactly the evidence needed for their documented purpose, at the appropriate disclosure level, within TTL constraints, with post-access accountability. It deepens Section 10 and Appendix Q with comprehensive profiles, query-safe views, and over-disclosure prevention controls.

X.1 Verification Output Taxonomy

Verification Output Taxonomy Table:

Output Type	Code	Disclosure Level	Content	Tier
Aggregate statistical report	OUT-AGG	Anonymized aggregate only	Pass rates, counts, distributions, trends	Tier 0
VOP (proof-based)	OUT-VOP	Bounded claim only	PASS/FAIL + freshness + revocation status	Tier 0 / Tier 1
Minimized disclosure extract	OUT-MIN	Pseudonymized, scoped	State values, evidence class presence, key dates	Tier 1
Scoped evidence extract	OUT-SCOPED	Pseudonymized, full artifact detail within scope	Complete evidence artifacts for specified subject	Tier 1
Full identity extract	OUT-FULL	De-pseudonymized within approved scope	Underlying identity, raw evidence, full detail	Tier 2
Replay reconstruction	OUT-REPLAY	Per replay tier	Complete state reconstruction at historical point	Tier 1 or Tier 2

X.2 Reviewer and Examiner Profile Taxonomy

Reviewer Profile Matrix:

Profile	Typical Purpose Codes	Default Tier	Upgrade Path
Routine operational auditor	PUR-EXAM-ROUTINE	Tier 0 → Tier 1	Documented finding triggers Tier 1 request
Break investigator	PUR-RECON-BREAK	Tier 1	Break severity SEV-1 may justify Tier 2
Safety incident investigator	PUR-SAFETY-INCIDENT	Tier 1 → Tier 2	Patient notification requirement triggers Tier 2
Recall scope coordinator	PUR-RECALL-SCOPE	Tier 1	Full custody identification may require Tier 2
Dispute resolution	PUR-DISPUTE	Tier 1	Identity of disputing parties

Profile	Typical Purpose Codes	Default Tier	Upgrade Path
authority			may require Tier 2
Regulatory enforcement investigator	PUR-ENFORCEMENT	Tier 1 → Tier 2	Enforcement action requires Tier 2 with dual-control
Governance reviewer (recertification)	PUR-EXAM-ROUTINE	Tier 0 → Tier 1	Deficiency finding triggers Tier 1

X.3 Minimal Disclosure Profiles

Minimal Disclosure Profile Matrix:

Evidence Domain	Tier 0 Disclosure	Tier 1 Disclosure	Tier 2 Disclosure
Product identity	Product category counts; authenticity pass rates	CPO reference, batch/lot, authenticity state, provenance status	Full manufacturer identity, commercial terms
Authorization	Authorization validity rates; override frequency	Authorization type, validity state, scope summary, issuer pseudonym	Prescriber identity, license details, practice address
Custody	Custody integrity rates; excursion frequencies	Chain status, event count, last event type/timestamp, custodian pseudonym	Custodian identity, facility details, transport specifics
Safety	Safety evidence coverage rates; override counts	Safety state, evidence class presence/absence, freshness, override flag	Patient parameters, clinical notes, raw decision inputs
Claims	Gate pass rates; adjustment rates; aging distribution	Claim status, gate results, amount category, temporal assessment	Patient identity, benefit plan specifics, pricing details
Reviewer access	Access volume by tier and purpose	Individual access event metadata (pseudonymized reviewer)	Reviewer identity, full accessed artifact list

X.4 Query-Safe Evidence Views

Query-Safe Evidence View Table:

View Name	Content	Excluded	Use Case
Product-Posture-View	Authenticity state, provenance status, recall status, last verification timestamp	Manufacturer commercial terms, pricing, supply chain partner identities	Routine product integrity review
Authorization-Lifecycle-View	Authorization type, validity state, issuer legitimacy state, bound summary, supersession position	Prescriber name, patient identity, clinical indication details	Authorization compliance audit
Custody-Chain-Summary-View	Chain status, event	Custodian	Custody integrity

View Name	Content	Excluded	Use Case
	count, last event, gap count, excursion count	commercial identity, facility address, transport routing	assessment
Safety-Coverage-View	Safety state, evidence class inventory (present/absent/stale), override flag, review posture	Patient parameters, clinical notes, raw algorithm inputs	Safety evidence completeness review
Dispensation-Gate-View	Gate results (G1–G7 PASS/FAIL), review posture, dispensation timestamp	Patient identity, full prescription details, clinical rationale (unless override)	Dispensation compliance verification
Claim-Status-View	Claim status, gate results (CG/EG), temporal assessment, amount category	Patient identity, benefit plan details, specific pricing	Claim adjudication audit

X.5 Sufficiency Standards for Review Purposes

Sufficiency Standard Matrix:

Review Purpose	Minimum Output Type	Minimum Tier	Sufficient When
Routine compliance audit	OUT-AGG + selected OUT-MIN	Tier 0 + Tier 1	Aggregate statistics within acceptable ranges; no material findings in sample
Break investigation	OUT-SCOPED for break-affected entities	Tier 1	Root cause identified; corrective action documented; break resolved
Safety incident investigation	OUT-SCOPED + potentially OUT-FULL for patient notification	Tier 1 + Tier 2 (if patient ID needed)	Clinical assessment complete; patient safety confirmed; corrective action documented
Recall scope determination	OUT-SCOPED for affected products and custody holders	Tier 1	All affected units identified; all custody holders notified
Recertification assessment	OUT-AGG + sampled OUT-MIN	Tier 0 + Tier 1	All recertification criteria evaluated; deficiencies documented with remediation plans

X.6 Purpose Limitation, TTL, and Escalation Rules

Purpose / TTL / Escalation Matrix:

Purpose Code	Default TTL	Renewal Process	Escalation to Tier 2 Trigger
PUR-EXAM-ROUTINE	30 days	Standard re-request	Material finding requiring identity verification

Purpose Code	Default TTL	Renewal Process	Escalation to Tier 2 Trigger
PUR-RECON-BREAK	14 days	Updated justification required	SEV-1 break with potential adversarial pattern
PUR-SAFETY-INCIDENT	30 days	Updated justification with clinical status	Patient notification requirement
PUR-RECALL-SCOPE	Duration of recall lifecycle	Automatic renewal while recall active	Custody holder identification for unresponsive entities
PUR-DISPUTE	Duration of dispute lifecycle	Automatic renewal while dispute active	Identity of parties needed for determination
PUR-ENFORCEMENT	Per regulatory authority	Re-authorization with updated scope	Standard Tier 2 controls (dual-control, objective trigger)

X.7 Reviewer-Safe Replay and Bounded Reconstruction

Reviewer-Safe Replay Matrix:

Replay Type	Disclosure Level	What Reviewer Sees	What Reviewer Does Not See
Product history replay	Tier 1	CPO versions, provenance chain events (pseudonymized actors), custody transitions, state changes	Manufacturer commercial arrangements, custodian identities, pricing
Authorization lifecycle replay	Tier 1	Authorization versions, EP Deltas, bound changes, supersession chain	Prescriber personal details, patient identity
Clinical decision replay	Tier 1	Decision state record, evidence class presence, algorithm version, override flag and justification	Patient parameters, raw clinical data, full prescriber identity
Claim lifecycle replay	Tier 1	Claim events, gate results, temporal assessment, adjustment chain	Patient identity, benefit plan terms, specific pricing

X.8 Post-Access Review and Access-Governance Controls

Post-Access Review Matrix:

Access Tier	PARP Required	PARP Contents	Review SLA	Non-Compliance Response
Tier 0	No (standard logging only)	N/A	N/A	N/A
Tier 1 (routine)	Optional per institutional policy	Scope verification, findings summary	Per institutional policy	Access pattern review
Tier 1 (sensitive)	Yes	Scope verification, data handling confirmation, findings summary	5 business days	Compliance alert at 10 days
Tier 2	Always	Full PARP per Section 10.6 (9 required fields)	5 business days	Governance notification at 7 days; compliance violation

Access Tier	PARP Required	PARP Contents	Review SLA	Non-Compliance Response
				at 10 days

X.9 Verification Failures and Over-Disclosure Prevention

Over-Disclosure Prevention Matrix:

Risk	Prevention Control	Detection Method	Response
Tier 0 output contains identifiable data	Automated anonymization check before output delivery	Pattern scan for identifiers, pseudonyms, or small-N aggregations	Output blocked; re-anonymized; incident logged
Tier 1 output contains de-pseudonymized identifiers	Pseudonymization verification at output generation	Identifier format check (real names, license numbers, addresses)	Output blocked; identifiers re-pseudonymized
Tier 2 output scope exceeds approval	Scope enforcement at retrieval: only approved artifact references retrievable	Artifact reference comparison against approval scope	Excess artifacts excluded; scope violation logged
Bulk export exceeding reasonable review volume	Export volume threshold monitoring	Volume anomaly detection	Export paused; reviewer contacted; governance notification if anomalous
Evidence retained by reviewer beyond TTL	TTL enforcement at access layer	Automated access revocation at TTL expiry	Access terminated; retention reminder sent

X.10 Minimal Proof-Based Verification Outputs (Optional)

Minimal Proof-Based Output Table:

Query	Traditional Output (Tier 1)	Proof-Based Output (VOP)	Disclosure Reduction
"Is product X authentic?"	Full PAES with provenance detail	VOP: PASS + freshness + revocation	Eliminates provenance chain detail exposure
"Is prescriber authorized?"	Full AES with credential detail	VOP: PASS + freshness + scope match	Eliminates credential and practice detail
"Is safety evidence sufficient?"	Full SES with evidence class detail	VOP: PASS + evidence class count + freshness	Eliminates clinical decision detail
"Has custody chain been verified?"	Full CES with event chain	VOP: PASS + event count + last event timestamp	Eliminates custodian identity and facility detail

X.11 Reviewer / Examiner Query Families

Reviewer / Examiner Query Family Table:

Family	Queries	Default Tier	Output Type
Product integrity queries	EQP-001 through EQP-003 (Appendix E)	Tier 1	OUT-SCOPED or OUT-VOP
Authorization compliance queries	EQP-004 through EQP-006	Tier 1	OUT-SCOPED
Dispensation gate queries	EQP-007 through EQP-008	Tier 1	OUT-SCOPED
Safety evidence queries	EQP-009 through EQP-011	Tier 1	OUT-SCOPED or OUT-VOP
Reconciliation queries	EQP-012 through EQP-014	Tier 0 / Tier 1	OUT-AGG or OUT-SCOPED
Access compliance queries	EQP-017 through EQP-018	Tier 0 / Tier 1	OUT-AGG or OUT-SCOPED

X.12 Offboarding, Portability, and Output Handoff Rules

Offboarding Output Handoff Matrix:

Output Type	Portable to Legacy	Handoff Requirement	Post-Handoff Access
Aggregate reports (OUT-AGG)	Yes	Standard data transfer	Archived in legacy reporting system
VOPs	Partial — legacy may not validate proofs	Archive VOP artifacts with integrity attestation	Retrieved from framework archive if needed
Minimized disclosure extracts	Yes — structured data	Standard data transfer with minimization log	Subject to legacy retention policy
Full evidence extracts	Per offboarding proof bundle procedures (Appendix I)	Content-addressed archive with integrity verification	Per archival retention schedule (Section 13.7)

X.13 Worked Mini-Scenarios

Worked Scenario Summary Table:

Scenario	Review Type	Tier Used	Output Type	Outcome
Routine quarterly audit: product authenticity pass rates	Compliance audit	Tier 0	OUT-AGG	99.7% pass rate; no material findings
Break investigation: custody gap for controlled substance	Break investigation	Tier 1	OUT-SCOPED	Gap caused by logistics system timeout; compensating evidence obtained; break resolved
Safety incident: contraindication override without	Safety investigation	Tier 1 → Tier 2	OUT-SCOPED → OUT-FULL (patient notification needed)	Override confirmed undocumented; clinical re-assessment confirms no harm;

Scenario	Review Type	Tier Used	Output Type	Outcome
documentation				DS-05 retroactively documented; process improvement initiated

X.14 Reader Action Map

Reader Profile	Start Here	Key Tables	Primary Actions
Access control implementer	X.3, X.6	Disclosure Profile Matrix; Purpose/TTL Matrix	Configure access tiers, purpose codes, TTL enforcement
Reviewer / examiner	X.4, X.5	Query-Safe View Table; Sufficiency Matrix	Select appropriate view; assess sufficiency for purpose
Privacy / compliance officer	X.9, X.8	Over-Disclosure Prevention Matrix; Post-Access Review Matrix	Monitor disclosure controls; review PARP completion
System designer	X.1, X.10	Output Taxonomy; Proof-Based Output Table	Design output generation layer; implement VOP capability

Appendix Y — Cross-Border Portability, Conflict-of-Process Handling, and Jurisdiction-Bounded Review

Y.0 Purpose and Reader Orientation

This appendix deepens Appendix R with a complete operational model for cross-border and cross-domain evidence portability. It addresses how evidence artifacts maintain coherence when products, authorizations, or review processes cross jurisdictional or institutional boundaries — without assuming legal harmonization.

Y.1 Portability Taxonomy

Portability Taxonomy Table:

Portability Type	Code	Description	Example
Product portability	PORT-PROD	Product manufactured in one jurisdiction; distributed/dispensed in another	Medicine manufactured in Jurisdiction B; dispensed in Jurisdiction A
Authorization portability	PORT-AUTH	Prescription issued in one jurisdiction; presented for dispensation in another	Prescription from Jurisdiction A presented at Jurisdiction B pharmacy
Evidence portability	PORT-EVID	Evidence artifacts generated under one framework/format transported to another	Foreign provenance manifest imported into framework
Review portability	PORT-REV	Reviewer in one jurisdiction accessing evidence generated in another	Jurisdiction A examiner reviewing dispensation evidence from Jurisdiction B
Claim portability	PORT-CLM	Claim for reimbursement crosses jurisdictional benefit boundaries	Cross-border healthcare reimbursement
Offboarding portability	PORT-OFFB	Evidence transitioned from framework to legacy system in different domain	Framework evidence archived; legacy system in different jurisdiction

---

Y.2 Cross-Border and Cross-Domain Transfer Principles

Transfer Principle Matrix:

Principle	Requirement	Violation Response
Evidence integrity preservation	Transferred evidence retains content-addressed integrity markers; hash verification at both source and destination	Integrity failure at destination → BRK-INTEG; transfer rejected or quarantined
Format conversion documentation	When evidence format is converted (e.g., foreign provenance format → framework manifest), the conversion is documented with mapping record	Undocumented conversion → evidence treated as CB-3 (Low Confidence) per Appendix S
Equivalence	Foreign credentials, evidence	No equivalence assessment →

Principle	Requirement	Violation Response
assessment	standards, or processes assessed for functional equivalence before reliance	issuer treated as ISSU_UNVERIFIED; evidence as CB-3
Jurisdiction-bounded disclosure	Evidence disclosed to foreign reviewer only under documented purpose, TTL, and applicable data transfer constraints	Cross-border disclosure without documented authority → access abuse (ABP-008 variant)
No automatic canonicalization	Foreign evidence does not automatically become canonical state in receiving jurisdiction; adoption requires explicit assessment	Foreign evidence treated as canonical without assessment → governance violation

Y.3 Jurisdiction-Bounded Review Model

Jurisdiction-Bounded Review Matrix:

Review Scenario	Jurisdiction A Reviewer	Jurisdiction B Evidence	Access Conditions
Product imported from B to A; A reviewer examines provenance	Access to provenance manifest (may be in B's format)	Provenance events from B custody chain	Tier 1 with cross-border purpose code; format conversion if needed; equivalence note
Prescription from A presented in B; B reviewer verifies authorization	Access to AES (generated under A's credentialing)	A's credential verification records	Tier 1; A credential treated as ISSU_UNVERIFIED unless equivalence established
Cross-border recall; both jurisdictions review scope	Each jurisdiction accesses own custody evidence	Counterpart jurisdiction provides scope determination	Tier 1 within each jurisdiction; cross-border information shared per documented agreement
Dispute involving parties in both jurisdictions	Each jurisdiction's dispute authority reviews own-jurisdiction evidence	Shared evidence per agreement	Tier 1 minimum; Tier 2 requires dual-control from both jurisdictions

Y.4 Conflict-of-Process Taxonomy

Conflict-of-Process Taxonomy Table:

Conflict Type	Code	Description	Resolution Approach
Format conflict	COP-FMT	Evidence generated in incompatible format; cannot be directly ingested	Format conversion with documented mapping; CB-3 confidence until corroborated
Standard conflict	COP-STD	Different evidence standards (continuous monitoring vs. periodic attestation)	Equivalence assessment; institutional quality acceptance; documented qualification
Temporal	COP-TMP	Different freshness windows	Apply stricter of the two standards;

Conflict Type	Code	Description	Resolution Approach
conflict		or validity period interpretations	document basis
Authority conflict	COP-ATH	Credential recognized in one jurisdiction but not another	ISSU_UNVERIFIED in receiving jurisdiction; supplemental verification or local re-authorization
Retention conflict	COP-RET	Different retention requirements across jurisdictions	Apply longer retention; document basis; monitor for changes
Disclosure conflict	COP-DIS	One jurisdiction requires disclosure that another prohibits	Minimized disclosure; proof-based verification where possible; documented legal constraint

Y.5 Portable Evidence Set and Handoff Requirements

Portable Evidence Set and Handoff Matrix:

Evidence Type	Portable Elements	Non-Portable Elements	Handoff Documentation
PAES (product)	CPO, batch/lot, provenance manifest, integrity markers	Manufacturer commercial terms, pricing arrangements	Format conversion record; equivalence assessment for manufacturer credential
AES (authorization)	Authorization type, validity state, scope summary	Prescriber personal details (unless Tier 2 authorized cross-border)	Credential equivalence assessment; scope verification against destination jurisdiction
CES (custody)	Custody event chain, handoff records, condition logs	Custodian commercial identity, facility addresses	Border transit events documented; custody gap coverage for transit period
SES (safety)	Product safety profile reference, evidence class presence	Patient-specific clinical data (non-portable by default)	Source data version mapping to destination jurisdiction equivalents
CLM-EP (claims)	Claim status, gate results	Benefit plan specifics, pricing details	Cross-border reimbursement agreement reference (if applicable)

Y.6 Current-Reference State, Historical State, and Parallel-State Management

Current-Reference / Historical / Parallel-State Matrix:

Scenario	State Management	Evidence Requirement
Product evidence imported; destination assigns own canonical state	Foreign evidence preserved as historical; destination evidence becomes canonical	Both versions retained; linkage documented
Authorization recognized cross-border with equivalence	Foreign authorization adopted as current-reference with equivalence flag	Equivalence assessment record; supplemental local verification
Conflicting safety assessments between	Parallel states maintained; dispensation uses destination	Both assessments preserved; dispensation references

Scenario	State Management	Evidence Requirement
jurisdictions	jurisdiction's assessment	destination SES
Recall issued in one jurisdiction; affects products in another	Both jurisdictions maintain their own recall state for affected products	Cross-border notification evidence; jurisdiction-specific disposition records

Y.7 Bounded Rebinding and Destination Adoption Logic

Destination Rebinding and Adoption Matrix:

Evidence Type	Adoption Condition	Rebinding Steps	Documentation
Product identity (CPO)	Product registered in destination product registry	Cross-reference mapping: source CPO ↔ destination product identifier	Mapping record with integrity verification
Issuer credential	Equivalence assessment confirms functional equivalence	Destination AES generated with equivalence_assessed flag	Equivalence assessment record
Custody chain	Border transit documented as explicit custody events	Source chain endpoint linked to destination chain entry via border transit events	Border transit custody event records
Safety evidence	Source data mapped to destination equivalents	Destination SES generated referencing destination formulary/interaction databases	Source-to-destination data mapping record

Y.8 Cross-Border Disputes, Holds, and Unresolved-State Carry-Forward

Cross-Border Dispute and Hold Matrix:

Situation	Jurisdiction A Action	Jurisdiction B Action	Coordination Requirement
Product hold in A; product already shipped to B	A issues hold notification to B	B applies hold-only containment on received units	Cross-border notification evidence; B acknowledges A's hold
Authorization disputed between jurisdictions	A holds pending dispensation under disputed authorization	B (if product is there) holds dispensation pending resolution	Dispute evidence shared per agreement; determination by competent authority
Recall in A; product distributed to B	A issues recall notification to B	B executes recall per own procedures for affected units	Consolidated recall tracking; per-jurisdiction disposition records
Unresolved break at border transit	Break carried forward as open in both jurisdictions	Both jurisdictions maintain break in open breaks register	Cross-border break coordination; resolution requires both jurisdictions to update

Y.9 Reviewer-Safe Verification and Minimal Disclosure Across Domains

Reviewer-Safe Cross-Domain Verification Matrix:

Cross-Domain Review	Disclosure Control	Minimum Output	Maximum Output
A reviewer examining B product evidence	B evidence disclosed at Tier 1 with pseudonymization per B's standards	Product-Posture-View (Appendix X)	Full PAES only under documented cross-border agreement and Tier 2 with B's approval
A reviewer examining B authorization	B credential details disclosed only if equivalence established and purpose documented	VOP confirming ISSU_CONFIRMED (if VOP available)	AES detail under Tier 2 with dual jurisdiction approval
Joint investigation (both jurisdictions)	Each jurisdiction discloses per own tiered access rules	Shared investigation summary with pseudonymized references	Full evidence sharing under formal cross-border investigation agreement

---

Y.10 Governance, Accountability, and Material Change Controls for Portability

Governance and Accountability Matrix:

Governance Activity	Responsible	Accountable	Evidence
Equivalence assessment	Receiving jurisdiction operational function	Receiving jurisdiction governance body	Equivalence assessment record; approval
Cross-border disclosure authorization	Both jurisdictions' access control functions	Both governance bodies	Documented agreement; access event logs
Border transit custody documentation	Transferring and receiving entities	Both jurisdictions' surveillance functions	Border transit custody events
Cross-border recall coordination	Recall authority (issuing jurisdiction)	Both jurisdictions' governance bodies	Recall notifications; acknowledgments; disposition records
Portability material change	Operational function detecting change	Governance body in affected jurisdiction	Material change trigger; governance response

---

Y.11 Reviewer / Examiner Query Families for Portability and Conflict Handling

Reviewer / Examiner Query Family Table:

Query	Purpose	Tier	Expected Output
"Show all cross-border evidence imports for period X"	Audit of foreign evidence adoption	Tier 1	List of imported evidence with equivalence assessment status
"Identify products with foreign provenance in dispensable inventory"	Product integrity review	Tier 1	Product list with provenance source jurisdiction and confidence band
"Show unresolved cross-border	Cross-border	Tier 1	Open holds with cross-border

Query	Purpose	Tier	Expected Output
holds"	containment review		origin and coordination status
"Verify equivalence assessments are current"	Equivalence freshness review	Tier 0 / Tier 1	Equivalence assessment aging report

Y.12 Offboarding, Legacy Compatibility, and Transition Closure

Offboarding and Transition Closure Matrix:

Portability Element	Transition Handling	Closure Condition
Cross-border evidence linkage	Archive cross-reference mappings; export linkage records to legacy	All cross-references documented; no orphaned linkages
Equivalence assessments	Archive assessments; export status to legacy	All active assessments documented; expiry dates noted
Open cross-border holds/breaks	Resolve or transfer per governance agreement; document in open breaks disclosure	All items resolved or transferred with accountability assignment
Cross-border notification channels	Decommission framework channels; establish legacy contact points	Contact handoff documented; both jurisdictions acknowledge

Y.13 Worked Mini-Scenarios

Worked Scenario Summary Table:

Scenario	Portability Type	Conflict	Resolution
Biologic imported from Jurisdiction B; storage monitoring was periodic attestation (not continuous)	PORT-PROD + COP-STD	Standard conflict: continuous vs. periodic monitoring	Institutional quality accepts B's standard with documented qualification; provenance COMPLETE with CB-2 confidence annotation
Patient travels from A to B with prescription; B pharmacy cannot verify A's prescriber credentials	PORT-AUTH + COP-ATH	Authority conflict: credential not recognized	Dispensation blocked; patient referred to local prescriber for B-jurisdiction prescription
Recall issued in A for batch distributed to A, B, and C	PORT-PROD (recall)	Multi-jurisdiction recall coordination	Framework recall record as canonical; jurisdiction-specific notifications and dispositions documented separately; consolidated closure requires all-jurisdiction accounting

Y.14 Reader Action Map

Reader Profile	Start Here	Key Tables	Primary Actions
Import/export	Y.5,	Portable Evidence Set Matrix;	Document handoff; perform

Reader Profile	Start Here	Key Tables	Primary Actions
coordinator	Y.7	Rebinding Matrix	equivalence assessment
Cross-border reviewer	Y.3, Y.9	Jurisdiction-Bounded Review Matrix; Cross-Domain Verification Matrix	Access foreign evidence per bounded rules
Governance (cross-border)	Y.10	Governance Matrix	Approve equivalence assessments; authorize cross-border disclosure
Recall coordinator (multi-jurisdiction)	Y.8	Cross-Border Dispute and Hold Matrix	Coordinate cross-jurisdiction recall response

Appendix Z — Performance, Service-Level Objectives, Operational Resilience, and Recovery Discipline

Z.0 Purpose and Reader Orientation

This appendix deepens Appendix T with operational resilience controls, degradation logic, backpressure handling, replay capacity, recovery discipline, and incident classification specific to healthcare workflow domains. It defines how the framework operates under stress and how it recovers.

Z.1 Performance Taxonomy by Workflow Class

Workflow Performance Taxonomy Table:

Workflow Class	Latency Sensitivity	Throughput Sensitivity	Integrity Sensitivity	Example
Dispensation gate evaluation	High — patient waiting	Moderate (batch capability for refills)	Critical — incorrect gate result is unsafe	Pharmacy dispensation at point of care
Provenance verification	Moderate — at receipt	Moderate (batch for shipment receipt)	Critical — counterfeit detection depends on it	Distributor receiving verification
Authorization verification	High — at dispensation	Low (per-transaction)	Critical — unauthorized dispensation	Prescription validity check at pharmacy
Safety evidence generation	Moderate — pre-dispensation	Low	Critical — decision safety depends on it	CDSS contraindication check
Reconciliation execution	Low — batch process	High (large artifact populations)	High — break detection depends on it	Daily custody-provenance alignment
Claim processing	Low–Moderate	High (volume-dependent)	High — financial integrity	Batch claim adjudication
Reviewer evidence retrieval	Low (SLO-bounded)	Low	High — evidence integrity	Examiner query response

---

Z.2 Service-Level Objectives and Timeliness Bands

SLO and Timeliness Band Matrix:

Workflow	Target Latency	Acceptable Degradation	Unacceptable Threshold
Dispensation gate (all gates)	<30 seconds total	<2 minutes (degraded mode)	>5 minutes — escalate to manual confirmation pathway
Provenance	<5 minutes per	<15 minutes	>30 minutes — accept with

Workflow	Target Latency	Acceptable Degradation	Unacceptable Threshold
verification at receipt	product unit		condition annotation; re-verify batch
Authorization freshness check	<10 seconds	<30 seconds	>2 minutes — conservative FAIL; hold pending re-check
Safety evidence generation (CDSS)	<15 seconds	<1 minute	>2 minutes — manual confirmation pathway activated
Reconciliation cycle	Within cadence window (daily/weekly)	+24 hours delay	+48 hours — governance notification; BRK-FRESH-005
Claim gate evaluation	<1 minute per claim	<5 minutes	>10 minutes — batch queue management
Evidence retrieval (standard)	<48 hours	<5 business days	>5 business days — governance escalation

Z.3 Observability and Integrity Signals

Observability and Integrity Signal Table:

Signal Category	Signals Monitored	Alert Threshold	Response
Gate performance	Gate evaluation latency, gate pass/fail rates, gate timeout frequency	Latency >2x target; pass rate drop >2% from baseline; timeout rate >1%	Performance investigation; capacity assessment
Evidence storage	Content-address verification pass rate, retrieval latency, replication lag	Any verification failure; retrieval >2x SLO; replication lag >threshold	Integrity investigation (BRK-INTEG); storage remediation
Reconciliation health	Reconciliation execution on time, break detection rate, break aging	Missed cycle; break rate spike >2x baseline; aging >SLA	Reconciliation priority; governance notification
Reviewer access	Access volume, TTL compliance, PARP completion rate	Volume anomaly; TTL overrun; PARP overdue	Access governance review
Claim pipeline	Claim aging, gate failure rate, adjustment rate	Aging >SLA; gate failure spike; adjustment rate >threshold	Pipeline investigation; capacity management

Z.4 Degraded Modes and Graceful Degradation Logic

Degraded Mode Matrix:

Component Failure	Degraded Mode	Capability Retained	Capability Lost	Restoration Trigger
Revocation service unavailable	Conservative FAIL for revocation checks	Dispensation via manual confirmation	Automated revocation verification	Service restored; queued re-checks processed

Component Failure	Degraded Mode	Capability Retained	Capability Lost	Restoration Trigger
	(per Baseline D)	pathway; hold-only on automated dispensation		
CDSS unavailable	Manual safety assessment pathway activated	Dispensation with pharmacist manual safety check (DS-05 documentation required)	Automated contraindication/interaction screening	CDSS restored; batch re-screening of manual-pathway dispensation
Evidence storage degraded	Read from replica; write queued	Evidence retrieval (from replica); evidence generation (queued)	Real-time write confirmation	Primary storage restored; queue drained
Reconciliation engine offline	Reconciliation deferred; manual break monitoring	Custody event logging continues; evidence generation continues	Automated reconciliation; break detection	Engine restored; catch-up reconciliation executed
Claim processing system degraded	Claim queue accumulates; priority processing for urgent claims	Claim submission; priority adjudication	Batch processing; aging monitoring	System restored; backlog processing initiated

Z.5 Backpressure, Queues, and Workload Management

Queue and Backpressure Management Matrix:

Queue	Normal Capacity	Backpressure Trigger	Backpressure Action	Priority Rule
Dispensation gate queue	Real-time (no queue)	>5 second latency sustained >5 minutes	Activate degraded mode; alert operations	Controlled substances and narrow therapeutic index prioritized
Reconciliation queue	Daily batch capacity	Queue depth >2x normal	Alert operations; defer non-critical reconciliation types	Provenance-custody alignment first; aggregate holdings second
Claim processing queue	Hourly batch capacity	Queue age >24 hours	Governance notification; expedited processing for aged claims	Claims approaching adjudication SLA processed first
Evidence retrieval queue	Per SLO capacity	Queue age >SLO target	Alert operations; increase retrieval resources	Emergency retrieval prioritized; standard deprioritized
Integrity verification queue	Continuous sampling capacity	Backlog >48 hours	Alert operations; prioritize critical evidence	Active dispensation evidence prioritized

Z.6 Evidence Continuity Under Stress

Evidence Continuity Under Stress Matrix:

Stress Condition	Evidence Generation	Evidence Storage	Evidence Retrieval	Reconciliation
High transaction volume spike	Continue generating; queue if needed	Write queue; no loss	May degrade to SLO+24h	Defer to next scheduled cycle
Storage system partial failure	Continue generating to queue	Queue writes; replicate to surviving nodes	Serve from replica	Continue if replica accessible
Network partition	Local generation continues; sync deferred	Local write; sync on reconnection	Local retrieval; remote unavailable	Deferred until partition healed; catch-up reconciliation
Multi-component failure	Minimal evidence generation (ILS only)	Emergency local storage	Emergency retrieval from local only	Suspended; post-recovery catch-up

---

Z.7 Replay Capacity and Reconstruction Readiness

Replay Capacity and Readiness Matrix:

Replay Type	Data Required	Storage Location	Readiness Target	Degraded Readiness
Product authenticity replay	CPO versions; PAES; provenance manifest	Content-addressed primary + replica	<1 hour retrieval for any product	<24 hours from replica
Authorization lifecycle replay	AES versions; EP Delta chain; supersession chain	Content-addressed primary + replica	<1 hour retrieval	<24 hours from replica
Custody chain replay	CES event chain; storage condition logs	Content-addressed primary + replica	<1 hour retrieval	<24 hours from replica
Clinical decision replay	Decision state records; referenced evidence classes; algorithm versions	Content-addressed primary + replica	<4 hours retrieval (includes version snapshots)	<48 hours
Full dispensation reconstruction	DEP-H + all upstream evidence sets	All evidence stores	<4 hours	<48 hours

---

Z.8 Restoration and Recovery Discipline

Restoration and Recovery Matrix:

Failure Type	Recovery Priority	RTO	RPO	Verification
Evidence storage failure	Critical	4 hours	15 minutes (replication)	Hash verification of all restored artifacts
Gate evaluation system	Critical	1 hour	Zero (stateless; re-	Test gate evaluation with known

Failure Type	Recovery Priority	RTO	RPO	Verification
failure			evaluate)	inputs
Reconciliation engine failure	High	24 hours	Last completed cycle	Catch-up reconciliation; break inventory comparison
CDSS failure	High	4 hours	Zero (re-query)	Test CDSS with known scenarios
Claim processing failure	Moderate	24 hours	Last processed batch	Queue reconciliation; claim count verification
Reviewer access system failure	Moderate	24 hours	Zero (access logs separate)	Access control verification

Z.9 Incident Classification and Escalation Logic

Incident Classification and Escalation Matrix:

Incident Category	Severity	Notification	Escalation
Evidence integrity failure (hash mismatch, silent overwrite)	SEV-1 (Critical)	Governance + regulatory liaison within 2 hours	Immediate containment; forensic investigation
Dispensation gate system failure (patients waiting)	SEV-1 (Critical)	Operations management immediately; governance within 1 hour	Manual confirmation pathway activated; capacity remediation
Reconciliation missed >2 consecutive cycles	SEV-2 (High)	Governance within 8 hours	Priority reconciliation; break risk assessment
Evidence storage degraded (replica serving)	SEV-2 (High)	Operations within 1 hour	Storage recovery; capacity assessment
Claim processing backlog >48 hours	SEV-3 (Moderate)	Operations management within 24 hours	Capacity increase; priority queue activation
Reviewer access system slow (>2x SLO)	SEV-3 (Moderate)	Operations within 24 hours	Performance investigation

Z.10 Governance, Change Control, and Materiality Triggers for Resilience

Governance and Materiality Trigger Matrix:

Trigger	Materiality Threshold	Governance Response	Documentation
SLO breach (any critical workflow)	Any single breach for dispensation/safety; 3+ breaches for others	Governance notification; root cause investigation	Incident record; RCA; remediation plan
Degraded mode activation	Any activation	Operations notification; governance if >4 hours	Degraded mode activation/deactivation records
Evidence integrity incident	Any instance	Immediate governance notification	PB per Appendix F; forensic investigation
Replay capacity below target	Any critical replay type below readiness target	Governance notification; capacity	Readiness assessment record

Trigger	Materiality Threshold	Governance Response	Documentation
		assessment	
Recovery time exceeds RTO	Any instance	Post-recovery governance review	Incident record; RTO gap analysis

Z.11 Reviewer / Examiner Visibility into Performance and Resilience State

Reviewer / Examiner Visibility Matrix:

Metric Category	Tier 0 Output	Tier 1 Output
Gate performance	Aggregate latency and pass rates	Per-dispensation-point gate performance; timeout incidents
Evidence integrity	Verification pass rate percentage	Individual integrity failure records
Reconciliation health	Cycle completion rate; break trend	Individual missed cycles; break aging details
Degraded mode events	Activation count and duration	Individual degraded mode records with affected scope
Claim pipeline health	Aggregate aging and throughput	Individual claim aging; backlog composition

Z.12 Closure Criteria and Post-Incident Review

Closure Criteria Matrix:

Incident Type	Closure Criteria	Post-Incident Review	Documentation
Evidence integrity incident	Valid version restored; dependent states re-verified; forensic complete	Mandatory within 10 business days	PB sealed; lessons learned; control improvement
System failure incident	Service restored within RTO; catch-up processing complete; no data loss beyond RPO	Within 5 business days	Incident record; RTO/RPO compliance; remediation
Degraded mode event	Normal mode restored; backlog cleared; evidence continuity verified	If duration >4 hours: within 5 business days	Degraded mode record; backlog processing log
SLO breach	Performance restored to target; root cause addressed	If repeated: governance review within 10 business days	Breach record; RCA; capacity plan

Z.13 Offboarding, Portability, and Resilience Carry-Forward

Offboarding and Resilience Carry-Forward Matrix:

Resilience Element	Carry-Forward Requirement	Legacy Expectation
SLO targets	Documented in offboarding proof bundle for reference	Legacy system maintains own SLOs
Degraded mode procedures	Documented; not directly portable	Legacy system defines own degradation

Resilience Element	Carry-Forward Requirement	Legacy Expectation
Replay capacity	All evidence archived per retention; replay capability preserved through archive	Archive retrieval SLO documented
Incident history	Incident records transferred as part of evidence archive	Available for post-offboarding investigation
Open incidents at offboarding	Resolved before offboarding or documented in open breaks disclosure	Accountability assigned per Section 13.6

Z.14 Worked Mini-Scenarios

Worked Scenario Summary Table:

Scenario	Stress Condition	Degraded Mode	Recovery	Closure
CDSS unavailable during morning dispensation peak	System failure	Manual safety assessment pathway for 2 hours; 47 dispensation events via manual confirmation	CDSS restored; batch re-screening of 47 events confirms no safety concern	Incident closed; RTO met (4h target; 2h actual); post-incident review documents cause (database connection pool exhaustion)
Evidence storage primary node failure	Storage failure	Replica serving reads; writes queued	Primary restored in 3 hours; queue drained in 1 hour; hash verification of all queued writes confirms integrity	Incident closed; RPO met (15min target; 8min actual replication lag)
Reconciliation engine offline for 36 hours (exceeds 24h acceptable delay)	Engine failure	Reconciliation deferred; manual break monitoring	Engine restored; catch-up reconciliation detects 2 SEV-3 breaks that accumulated during outage	Breaks resolved per standard workflow; governance notified of SLO breach; capacity improvement planned

Z.15 Reader Action Map

Reader Profile	Start Here	Key Tables	Primary Actions
Operations / SRE	Z.4–Z.5	Degraded Mode Matrix; Queue Matrix	Implement degradation logic; configure backpressure
Incident responder	Z.9, Z.8	Incident Classification Matrix; Recovery Matrix	Classify incident; execute recovery
Governance	Z.10, Z.12	Materiality Trigger Matrix; Closure Criteria	Review incidents; approve remediation
Examiner	Z.11, Z.2	Visibility Matrix; SLO Matrix	Assess operational resilience; verify SLO compliance

Appendix AA — Applied Operational Scenarios and Benefit Realization Across Medicines, Health Products, and Clinical Decisions

AA.0 Purpose and Reader Orientation

This appendix translates the framework into concrete operational scenarios showing practical benefits. Each scenario is fictional and demonstrates how multiple framework components interact to produce tangible improvements over status-quo healthcare workflows.

AA.1 How to Read the Scenarios

Each scenario includes: a setup describing the operational context, a workflow table showing step-by-step evidence flow, a "without framework" comparison showing what happens without the framework's controls, a "with framework" description showing improved handling, and a benefit summary.

AA.2 Scenario Design Principles

Scenario Design Principles Table:

Principle	Application
Realistic complexity	Each scenario involves multiple framework domains interacting
No real entities	All hospitals, pharmacies, manufacturers, prescribers, and patients are fictional
Evidence-centric	Every benefit traces to specific evidence artifacts, gates, or controls
Non-promotional	Scenarios show operational improvements, not ideological advocacy
Failure-inclusive	Scenarios include failures, holds, and corrections — not only happy paths
Reviewer-accessible	Each scenario shows how an examiner would verify the outcome

---

AA.3 Applied Scenario 1 — Medicine Release, Provenance Break Risk, and Hold-Only Containment

Setup. Regional Distributor RD-North receives 3,000 units of Product Alpha (a biologic) from Manufacturer PharmaCo. At receiving verification, 2,950 units pass CPO verification. 50 units show a hash chain break in the provenance manifest at the packaging stage.

Scenario 1 Workflow Table:

Step	Without Framework	With Framework	Evidence Produced
Receipt	Visual inspection only; all 3,000 units accepted	Automated CPO + provenance verification; 2,950 PASS; 50 flagged with BRK-PROV-002	CUS_RECEIPT with verification results; BRK detection record

Step	Without Framework	With Framework	Evidence Produced
Containment	No containment mechanism; all units enter dispensable inventory	Hold-only on 50 flagged units; 2,950 proceed normally	CUS_HOLD_ENTRY for 50 units; 2,950 units proceed through standard custody chain
Investigation	If problem discovered later: manual investigation across paper records	Automated hash chain analysis identifies packaging stage as break point; Manufacturer contacted	Investigation record; manufacturer query
Resolution	Slow; evidence scattered; may result in entire shipment quarantine	Manufacturer confirms: 50 units had packaging system error (label printed before system hash committed); provides corrected hash chain	Correction EP Delta; manufacturer attestation
Release	Delayed for entire shipment; or no investigation if problem not detected	50 units released after correction verified; 2,950 units never delayed	CUS_HOLD_RELEASE for 50; correction evidence preserved
Examiner verification	"How do I know these products are authentic?" — limited to paper certificates of analysis	Examiner runs EQP-001: complete provenance chain for any unit; EQP-003: full chain replay with integrity verification at each link	Examiner query results with evidence references

Benefit: 2,950 units experienced zero delay. 50 units contained and resolved in hours, not days. Complete evidence trail preserved. Examiner can independently verify any unit's authenticity.

AA.4 Applied Scenario 2 — Prescription Legitimacy, Expiry / Revocation Ambiguity, and Bounded Reviewer Escalation

Setup. Pharmacy BetaRx receives a refill request for Patient M's chronic medication (Product Gamma, 90-day supply). Gate G2 flags the prescription: prescriber Dr. Torres's credential was updated 12 days ago with an ambiguous update type.

Scenario 2 Workflow Table:

Step	Without Framework	With Framework	Evidence Produced
Refill request	Pharmacy checks prescription on file; assumes still valid	Gate G2: AES retrieved; credential update detected; type = AMBIGUOUS	Gate G2 PENDED result
Investigation	Pharmacist calls prescriber office; may take hours or days; no documentation	Tier 1 access: reviewer examines AES (pseudonymized); determines credential update was scope restriction	Tier 1 access record; review finding

Step	Without Framework	With Framework	Evidence Produced
Resolution	If prescriber unreachable: dispensation may proceed on assumption, or patient denied	Prescription held; prescriber confirms scope restriction; refers to Dr. Chen for Product Gamma; Dr. Chen issues new prescription	Supersession record; new AES for Dr. Chen
Dispensation	Dispensed under potentially invalid authority; or patient denied without clear explanation	All gates pass under Dr. Chen's prescription; dispensation proceeds	DEP-H with complete gate results
Post-event	No audit trail of investigation or resolution	Complete evidence: original gate failure, Tier 1 investigation, supersession, new authorization, successful dispensation	Full audit trail; PARP for Tier 1 access

Benefit: Patient received medication without undue delay. Potentially invalid dispensation prevented. Complete audit trail of decision-making preserved. Examiner can verify the entire escalation chain.

AA.5 Applied Scenario 3 — Controlled Dispensation with Custody Conflict and Correction Path

Setup. Hospital Delta's automated dispensing cabinet shows 20 units of Product Sigma (a controlled substance). The pharmacy management system shows 22 units. Gate G4 (custody integrity) fails for the next dispensation request due to the 2-unit discrepancy.

Scenario 3 Workflow Table:

Step	Without Framework	With Framework	Evidence Produced
Discrepancy detection	Discovered during manual monthly count; 2 units of controlled substance unaccounted for	BRK-CUST-004 detected at dispensation attempt; SEV-2 (controlled substance, >0 variance)	Break detection record; custody evidence showing discrepancy
Containment	Cabinet may continue dispensing while investigation proceeds	Hold-only on Product Sigma dispensation from this cabinet; other products unaffected	CUS_HOLD_ENTRY scoped to Product Sigma at this cabinet
Investigation	Paper-based count sheets reviewed; may take days	Custody event chain replay: CES shows 22 units received (CUS_RECEIPT); 0 units dispensed since last reconciliation; cabinet sensor log shows 20 units	Investigation record; CES replay results; sensor log cross-reference
Root cause	Difficult to determine with confidence	Investigation reveals: 2 units removed for emergency kit restocking without logging custody event; nurse confirms	Root cause: missing CUS_HANDOFF event; nurse statement

Step	Without Framework	With Framework	Evidence Produced
Correction	Informal adjustment; documentation gaps	Correction EP Delta: CES updated with retroactive CUS_HANDOFF for 2 units to emergency kit; approval from pharmacy director + nursing supervisor	Correction EP Delta with approval chain; retroactive custody event
Release	No formal release process	Hold released after correction verified; post-correction reconciliation confirms alignment (20 + 2 = 22)	CUS_HOLD_RELEASE; reconciliation report

Benefit: Controlled substance discrepancy detected immediately (not at monthly count). Root cause identified in hours. Correction documented with dual-authority approval. Complete evidence trail for DEA or institutional audit.

AA.6 Applied Scenario 4 — High-Impact Clinical Decision Support Review Under Minimal Disclosure Constraints

Setup. Hospital Delta's CDSS generates a dosage alert for Patient K: the calculated dose of Product Omega (narrow therapeutic index) is 15% above the standard maximum. Dr. Patel overrides the alert with documented clinical rationale (patient weight and renal function justify higher dose). Six months later, a quality review examines override patterns.

Scenario 4 Workflow Table:

Step	Without Framework	With Framework	Evidence Produced
Alert generation	Alert generated; may or may not be logged	SAFETY_ALERT_GENERATED logged; DS-01 contraindication check references IntDB-v2026.06	Alert ILS record; DS-01 with database version reference
Override	Override may be click-through with no documentation	Context-bound decision state generated with all evidence classes; DS-05 clinical rationale documented; Exceptional review posture assigned	Decision state record (Section 7.3) with all required fields
Dispensation	Dispensed; override may not be linked to dispensation record	DEP-H generated; gate G5 passes with override documentation; Exceptional review posture flagged	DEP-H with SES reference including override; review posture flag
Quality review (T+6 months)	Reviewer requests full patient records; privacy concerns; slow process	Tier 1 access: reviewer sees override frequency for CDSS version (Tier 0: aggregate), then examines specific decision states (Tier 1: pseudonymized); no patient identity	Tier 0 report: 23 overrides in 6 months; Tier 1: specific decision state records
Finding	Finding based on incomplete	Reviewer confirms: CDSS-v4.2 was current at override time; IntDB-v2026.06 was	Review finding record; PARP

Step	Without Framework	With Framework	Evidence Produced
	records; no version tracking	current; override rationale documented and clinically appropriate	documenting scope and findings
Outcome	Unclear audit trail; potential compliance exposure	Complete evidence: alert, override, rationale, dispensation, quality review — all linked and replayable; no patient identity exposed during quality review	Full evidence chain preserved; no privacy violation

Benefit: Quality review conducted with full clinical decision context but no patient identity exposure. Algorithm version tracking confirms override was assessed against current safety data. Complete evidence trail for institutional accreditation or regulatory examination.

AA.7 Cross-Scenario Benefit Matrix

Cross-Scenario Benefit Matrix:

Benefit Category	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Faster detection	Provenance break at receipt (minutes vs. post-incident)	Credential issue at refill (seconds vs. days)	Custody discrepancy at dispensation (immediate vs. monthly count)	Override documented at decision time (immediate vs. retrospective)
Proportional containment	50 units held; 2,950 unaffected	Single refill held; other dispensation unaffected	Single product at single cabinet; other inventory unaffected	Single decision flagged; other dispensation unaffected
Evidence completeness	Full provenance chain for every unit	Full authorization lifecycle with supersession	Complete custody audit trail with correction	Complete decision context with version tracking
Reviewer access	Examiner verifies any unit independently	Examiner traces full escalation chain	Examiner replays custody chain with correction	Examiner reviews without patient identity
Patient impact	No delay for 2,950 units	Patient received medication via authorized pathway	Controlled substance properly accounted	Clinical rationale documented for ongoing care

---

AA.8 Before / After Operational Comparison

Before / After Operational Comparison Table:

Operational Dimension	Before Framework	After Framework
Product authenticity verification	Paper certificates; visual inspection; post-incident investigation	Automated CPO + provenance verification at every receipt; real-time break detection
Authorization	Phone calls; assumption-based	Automated gate evaluation; structured

Operational Dimension	Before Framework	After Framework
verification	dispensation; paper trail	escalation; evidence-linked supersession
Custody integrity	Monthly manual counts; delayed detection; paper-based reconciliation	Continuous reconciliation; immediate break detection; content-addressed custody chain
Clinical decision accountability	Click-through overrides; no version tracking; retrospective chart review	Context-bound decision states; algorithm version tracking; reviewer-safe replay
Examiner access	Ad hoc evidence gathering; inconsistent formats; weeks for retrieval	Standardized evidence packs; query families; tiered access with SLOs
Correction discipline	Informal adjustments; overwritten records; no audit trail	Non-destructive correction with EP Delta; approval chain; prior state preserved
Recall management	Phone/fax notification; manual tracking; uncertain scope	Content-addressed recall tracking; aggregation hierarchy traversal; closure with 100% accountability

AA.9 Reviewer / Examiner Walkthrough View

Reviewer / Examiner Walkthrough Matrix:

Examiner Task	Scenario 1 Path	Scenario 2 Path	Scenario 3 Path	Scenario 4 Path
Verify operational state	EQP-001: authenticity state	EQP-004: authorization lifecycle	EQP-003: custody chain replay	EQP-010: decision state replay
Verify containment was proportional	Break record scope; hold scope; release evidence	Gate failure scope; hold scope; supersession evidence	Break scope (single cabinet); hold scope; correction approval	Override documentation; review posture; PARP
Verify resolution was proper	Correction EP Delta; manufacturer attestation; post-correction reconciliation	New AES; new prescription; gate re-evaluation	Correction EP Delta with dual approval; post-correction reconciliation	Decision state preserved; quality review finding documented
Access tier used	Tier 1 (break investigation)	Tier 1 (authorization review)	Tier 1 (custody investigation)	Tier 0 (aggregate) + Tier 1 (specific decision states)

AA.10 Break, Containment, and Correction Summary

Break / Containment / Correction Matrix:

Scenario	Break Code	Severity	Containment Scope	Resolution	EP Delta
1	BRK-PROV-002	SEV-2	50 units (of 3,000)	Manufacturer correction; hash	Provenance manifest

Scenario	Break Code	Severity	Containment Scope	Resolution	EP Delta
				chain repaired	correction
2	BRK-AUTH-005 (scope mismatch)	SEV-2	Single refill event	Prescriber transfer; new authorization	Supersession (original → new prescription)
3	BRK-CUST-004	SEV-2	Single product at single cabinet	Retroactive custody event; dual-authority correction	CES correction with approval chain
4	BRK-SAFE-003 (override without documentation)	N/A (override was documented)	N/A (no break; proper documentation)	Quality review confirms adequacy	N/A (no correction needed)

AA.11 Practical Benefit Realization by Stakeholder Type

Stakeholder Benefit Matrix:

Stakeholder	Primary Benefit	Evidence of Benefit
Patient	Receives authenticated product via authorized pathway with documented safety evidence; not denied due to unnecessary holds	Proportional containment scope; dispensation proceeds when evidence supports
Pharmacist / dispenser	Clear gate logic; documented authority to dispense or hold; protection from unauthorized dispensation liability	DEP-H with complete gate results; accountability insert
Prescriber	Credential issues detected before patient impact; structured override documentation protects clinical autonomy	AES lifecycle; DS-05 preservation; decision state record
Hospital / institution	Controlled substance accountability; clinical decision audit readiness; reduced examination burden	Custody chain evidence; decision state replay; standardized evidence packs
Distributor / manufacturer	Proportional containment (not entire shipment quarantine for isolated break); faster resolution	PAES per product unit; correction EP Delta with manufacturer attestation
Examiner / auditor	Standardized query families; tiered access; evidence integrity verification; SLO-bounded retrieval	Evidence packs per Appendix B; query pack per Appendix E; SLOs per Appendix T/Z
Benefit administrator	Evidence-linked claim gating; temporal assessment; dispute-resilient payout controls	CLM-EP with gate results; temporal assessment record; open breaks register
Governance body	Clear accountability (RACI); materiality triggers; structured escalation; no-master-key posture	Accountability inserts; governance records; recertification evidence

AA.12 Minimal Adoption Pathways

Minimal Adoption Pathway Table:

Adoption Level	Components Implemented	Benefit Achieved	Prerequisite
Level 1: Product identity	CPO registration; PAES generation; basic provenance manifest	Product authenticity verification at receipt; counterfeit detection capability	Product registration in framework
Level 2: + Authorization	AES generation; prescription lifecycle tracking; dispensation gates G1–G2	Authorization verification at dispensation; expired/revoked prescription detection	Level 1 + issuer credential integration
Level 3: + Custody	CES generation; custody event logging; gates G3–G4	Custody chain integrity; storage condition monitoring; handoff verification	Level 2 + custody event instrumentation
Level 4: + Safety	SES generation; decision state records; gates G5–G6	Proof-of-safety documentation; clinical decision replay; override accountability	Level 3 + clinical system integration
Level 5: + Claims	CLM-EP; claim gates; temporal assessment	Evidence-linked reimbursement; dispute-resilient payout	Level 4 + benefit administrator integration
Level 6: + Full governance	Complete reconciliation; tiered access; offboarding; recertification	Full operational evidence layer with examiner readiness	Level 5 + governance implementation

AA.13 Worked Mini-Outputs and Artifact Snapshots

Worked Output Snapshot Table:

Artifact	Scenario	Key Fields Shown	Purpose
BRK-PROV-002 detection record	Scenario 1	break_id, severity (SEV-2), affected_units (50), chain_break_position (packaging stage), detection_timestamp	Shows how provenance break is captured and scoped
Gate G2 PENDED result	Scenario 2	gate_id (G2), result (PENDED), reason (ISSUER_CREDENTIAL_UPDATE_AMBIGUOUS), dispensation_event_ref	Shows how ambiguous credential update blocks dispensation appropriately
Correction EP Delta for custody	Scenario 3	delta_id, previous_state (22 units at cabinet), new_state (20 at cabinet + 2 at emergency kit), correction_authority (pharmacy_director + nursing_supervisor), approval_timestamps	Shows non-destructive correction with dual-authority approval
Context-bound decision state	Scenario 4	decision_id, override_flag (true), algorithm_version (CDSS-v4.2), DS-05 rationale summary, review_posture (EXCEPTIONAL)	Shows how clinical decision context is preserved for reviewer-safe replay

AA.14 Reader Action Map

Reader Action Map:

Reader Profile	Start Here	Key Tables	Primary Actions
Executive / sponsor	AA.7, AA.8	Cross-Scenario Benefit Matrix; Before/After Table	Understand practical value proposition
Implementer	AA.12	Minimal Adoption Pathway Table	Plan phased implementation
Operator (pharmacy, distributor)	AA.3–AA.6	Scenario Workflow Tables	Understand operational impact of framework adoption
Examiner / auditor	AA.9	Reviewer Walkthrough Matrix	Understand verification approach across scenarios
Governance body	AA.11	Stakeholder Benefit Matrix	Assess benefit distribution; justify investment

---

Appendix AB — Minimal Institution Adoption Blueprint and Phased Implementation Path for Product Authenticity, Authorization, Custody, Proof-of-Safety, and Bounded Review Workflows

AB.0 Purpose and Reader Orientation

> *"The full framework need not be adopted all at once to produce meaningful operational benefit. Institutions can realize material improvements through a phased implementation path that begins with minimum viable authenticity, authorization, custody, and evidence controls, then progressively adds bounded verification, correction discipline, portability, resilience, and optional financially consequential workflows."*

This appendix provides an operational blueprint for phased adoption. It exists because the full framework — Sections 0–15 and Appendices A–AA — defines a comprehensive target architecture. No institution can or should implement every control simultaneously. Phased adoption sequences implementation to maximize early benefit while preserving architectural coherence and avoiding governance gaps.

> *"The objective of phased adoption is not to dilute the target architecture, but to sequence implementation in a way that preserves evidentiary integrity, reviewer usability, governance discipline, and reversibility while reducing operational disruption and premature complexity."*

What this appendix is: A phased operating blueprint for incremental adoption, with dependency logic, transition gates, minimum control sets, and governance-by-phase.

What this appendix is not: A vendor implementation plan, budget memo, procurement roadmap, staffing model, or generic digital-transformation playbook.

AB.1 Adoption Design Principles

Adoption Design Principles Table:

Principle	Operational Meaning	Anti-Pattern It Prevents
Minimum viable control first	Begin with the smallest control set that produces verifiable evidence and hold-only containment capability	Scope overload; "boil the ocean" implementation paralysis
Evidence before automation	Generate evidence artifacts (ILS, content-addressed records) before automating decision gates	Automated decisions on unverifiable inputs; opaque trust
Bounded review before broad disclosure	Implement tiered access and purpose limitation before expanding evidence access scope	Pervasive disclosure; surveillance creep; privacy violation
Preservation before	Implement non-destructive EP Delta discipline	Silent overwrites; lost audit

Principle	Operational Meaning	Anti-Pattern It Prevents
destructive correction	before any correction capability	trails; governance violations
Phased governance before scale	Establish minimal governance (approval chains, RACI, change control) before expanding participant count or transaction volume	Ungoverned scale; accountability gaps; incident paralysis
Reversibility from the start	Design offboarding and legacy compatibility into Phase 1; do not defer to later phases	Lock-in; lossy migration; inability to exit the framework
No big-bang dependency	Each phase produces standalone benefit; no phase requires completion of all prior controls	All-or-nothing risk; delayed benefit realization
Additive layering, not replacement	Each phase adds capability to the prior phase; no phase replaces or invalidates prior work	Rework; sunk cost; architectural inconsistency

AB.2 Institutional Starting Point Taxonomy

Institutions enter the framework from different operational maturity states. This taxonomy helps institutions identify their starting position and select the appropriate entry path.

Institutional Starting Point Taxonomy Table:

Starting Point	Code	Characteristics	Typical Entry Phase	Key Gap
Low-structure legacy	SP-LOW	Paper-based or ad-hoc digital records; no content addressing; no standardized evidence; no formal reconciliation	Phase 1 (full minimum viable set)	Everything — evidence generation, custody logging, governance structure
Partially controlled digital	SP-PART	Some digital tracking (e.g., electronic prescribing, barcode scanning) but no content-addressed evidence; inconsistent logging; limited reconciliation	Phase 1 (accelerated — some capabilities already present)	Content addressing; evidence integrity; reconciliation discipline; bounded review
High-control but fragmented	SP-FRAG	Strong controls in individual domains (e.g., good pharmacy systems, good warehouse management) but no cross-domain evidence linkage or unified reconciliation	Phase 2 entry (some Phase 1 controls already met)	Cross-domain evidence linkage; unified reconciliation; reviewer-safe outputs
Bounded-review-capable, weak custody	SP-BREV	Good access controls and reviewer discipline (e.g., tiered access, audit logging) but weak physical custody chain evidence	Phase 1 for custody; Phase 3 entry for reviewer controls	Custody event logging; provenance chain; storage condition monitoring

Starting Point	Code	Characteristics	Typical Entry Phase	Key Gap
Financially consequential workflow environment	SP-FIN	Claims and reimbursement systems operational but not evidence-linked to upstream product, authorization, or safety states	Phase 2–3 for core controls; Phase 4 for financial integration	Evidence linkage between claims and upstream domains; temporal assessment

Entry Path Guidance: Institutions assess their starting point, identify which Phase 1 controls they already satisfy, and focus Phase 1 implementation on remaining gaps. No institution is required to start from zero — existing capabilities are credited where they meet the evidence and governance requirements of the applicable phase.

AB.3 Minimum Viable Control Set (Phase 1)

Phase 1 defines the minimum set of controls that produce meaningful operational benefit: verifiable product identity, basic authorization checking, minimal custody logging, hold-only containment capability, and evidence generation.

Minimum Viable Control Set Matrix:

Control Domain	Phase 1 Minimum	Evidence Artifact	Reviewer Capability	What Phase 1 Cannot Do
Product authenticity	CPO registration for products in scope; basic manufacturer identity reference	CPO record (content-addressed); PAES (partial — CPO + manufacturer reference)	Product identity verification query	Full provenance chain replay; aggregation hierarchy traversal; cross-batch analysis
Provenance	Basic provenance linkage: manufacturer release → receipt at institution; not full multi-node chain	Provenance manifest (2-node: origin → institution)	Origin verification query	Multi-hop provenance replay; repackaging tracking; storage condition chain
Authorization	AES generation at dispensation; issuer legitimacy check (current credential status); basic scope match	AES record with credential reference and revocation check result	Authorization validity query at dispensation time	Supersession chain management; delegation chain verification; freshness-window enforcement
Custody	Minimum custody event logging: CUS_RECEIPT, CUS_DISPENSATION, CUS_HOLD_ENTRY, CUS_HOLD_RELEASE	ILS records for logged custody events; CES (partial)	Basic custody event query	Full chain replay; storage condition monitoring; excursion management; handoff pair matching

Control Domain	Phase 1 Minimum	Evidence Artifact	Reviewer Capability	What Phase 1 Cannot Do
Hold-only containment	Hold-only capability for products with evidence concerns; basic hold-set record	CUS_HOLD_ENTRY / CUS_HOLD_RELEASE records	Hold inventory query	Automated hold triggers; severity-based containment; preservation bundle generation
Evidence generation	Minimal evidence pack: PAES (partial), AES, custody ILS records; content-addressed manifest for generated artifacts	Evidence pack manifest (content-addressed)	Basic evidence retrieval	Full evidence pack per Appendix B templates; cross-domain linkage; reconciliation reports
Governance	Minimal approval chain: dual authorization for holds and corrections; basic RACI for core activities	Approval chain records; RACI documentation	Governance structure query	Full governance body structure; change control board; recertification cycles; material change triggers
Preservation	Basic preservation: content-addressed storage for generated artifacts; no deletion of evidence during retention period	Content-addressed artifact inventory	Artifact integrity verification	Full preservation bundles; legal hold capability; incident-specific preservation
Reviewer output	Basic reviewer-safe output: query-safe views for product identity, authorization status, and hold inventory	Tier 0 aggregate reports; basic Tier 1 scoped extracts	Basic examiner queries (EQP-001, EQP-004 simplified)	Full minimal disclosure profiles; VOP capability; post-access review; PARP

Phase 1 Operational Benefits:

- Product authenticity verification at receipt (counterfeit detection capability).
- Authorization verification at dispensation (expired/revoked prescription detection).
- Hold-only containment for evidence concerns (proportional response).
- Basic evidence trail for examiner queries (evidence-backed answers vs. assertions).
- Preservation of generated evidence (no evidence loss).

Phase 1 Limitations (Accepted):

- No full provenance chain replay beyond origin → institution.
- No automated reconciliation or break detection.
- No supersession chain management.
- No storage condition monitoring integration.
- No claim/reimbursement evidence linkage.
- No cross-domain portability.
- Limited reviewer access governance (basic Tier 0/1 only).

AB.4 Controlled Operational Expansion (Phase 2)

Phase 2 adds reconciliation, stronger custody continuity, correction discipline, and more mature evidence linkage. It builds on Phase 1 controls without replacing them.

Phase 2 Expansion Matrix:

Control Domain	Phase 2 Addition	New Evidence Artifacts	New Reviewer Capability	Transition Dependency
Provenance	Multi-node provenance chain; hash-chained event linkage; handoff pair matching	Full provenance manifest (content-addressed, hash-chained)	Provenance chain replay (EQP-003)	Phase 1 CPO and basic provenance in place
Custody	Full custody event taxonomy (Section 6.1); storage condition logging; excursion detection and assessment	Complete CES; storage condition logs; excursion records	Full custody chain replay; excursion history	Phase 1 custody logging operational
Reconciliation	Scheduled reconciliation for provenance-custody alignment and authorization-dispensation alignment	Reconciliation execution reports; break detection records	Break inventory queries (EQP-012); reconciliation cadence verification (EQP-014)	Phase 1 evidence artifacts available for reconciliation
Break management	Break taxonomy (Appendix C) applied; severity classification; containment per severity	Break lifecycle records (DETECTED → CONTAINED → INVESTIGATED → RESOLVED → CLOSED)	Break lifecycle queries; trend analysis (EQP-013)	Reconciliation operational (this phase)
Correction / supersession	EP Delta discipline for all corrections; non-destructive preservation; basic supersession chains	EP Delta records; version lineage records	Authorization lifecycle replay (EQP-004); version history queries	Phase 1 evidence generation; Phase 2 reconciliation
State determination	Canonical state determination logic (Appendix V); current-reference state vs. historical state	Canonical state records; supersession chain records	Canonical state queries (Appendix V, V.11)	Phase 2 supersession discipline
Governance	Change control procedures; recertification cadence (annual minimum); material change trigger	Change control records; recertification records; material change event records	Governance compliance queries (GOVN-001, GOVN-002)	Phase 1 minimal governance

Control Domain	Phase 2 Addition	New Evidence Artifacts	New Reviewer Capability	Transition Dependency
	documentation			
Preservation	Full preservation bundles for SEV-1 and SEV-2 breaks; legal hold capability	Preservation bundles per Appendix F templates	PB retrieval; legal hold inventory	Phase 1 content-addressed storage; Phase 2 break management

Phase 1 → Phase 2 Transition Criteria:

Criterion	Minimum Threshold	Evidence
Phase 1 controls operational	All Phase 1 minimum controls implemented and generating evidence	Phase 1 control inventory with evidence artifact samples
Evidence generation consistent	≥95% of dispensation events have associated PAES and AES records	Evidence coverage report
Hold-only capability tested	At least one hold-only exercise completed successfully (live or tabletop)	Hold exercise record with results
Preservation baseline met	Content-addressed storage operational; no evidence artifacts deleted during retention period	Storage integrity verification report
Governance minimum met	Dual-authorization for holds and corrections operational; basic RACI documented	Approval chain samples; RACI document
Governance approval for Phase 2	Governance body approves Phase 2 expansion	Governance approval record

---

AB.5 Reviewer and Examiner Readiness Buildout (Phase 3)

Phase 3 transforms the institution from "digitally tracked" to "reviewer-ready" — meaning an examiner can independently verify operational states through standardized evidence, bounded access, and replay capability.

Phase 3 Reviewer / Examiner Readiness Matrix:

Capability	Phase 3 Addition	Evidence	Readiness Indicator
Minimal disclosure profiles	Tier 0/1/2 disclosure profiles per Appendix X; pseudonymization at Tier 1; full identity only at Tier 2	Disclosure profile configuration; sample outputs per tier	Examiner receives appropriate detail per tier; no over-disclosure
Query-safe evidence views	Pre-defined evidence views (Appendix X, X.4) for product, authorization, custody, safety, dispensation, claims	View definitions; sample query results	Examiner queries return structured, scoped results — not raw data dumps
Reviewer-safe replay	Complete replay capability for product authenticity, authorization lifecycle, custody chain, and dispensation reconstruction	Replay execution records; sample replay outputs per replay type (Section 9.9)	Examiner can reconstruct any operational state at any historical point
Post-access review	PARP discipline for all Tier 2	PARP records; scope	Every Tier 2 access

Capability	Phase 3 Addition	Evidence	Readiness Indicator
	access and selected Tier 1 access; independent reviewer verification of scope compliance	verification documentation	event has completed PARP within SLA
Standard checks pack	Full checks pack (Appendix D) implemented and executable	Check execution records; pass/fail results per check	≥90% of applicable checks executable; failures documented with remediation
Examiner query pack	Full query pack (Appendix E) adapted to institutional retrieval infrastructure	Query execution samples; result format documentation	Examiner queries produce consistent, complete, integrity-verified results
Evidence retrieval SLOs	Retrieval SLOs operational per Appendix T	SLO compliance records	Standard queries responded within 48 hours; emergency within 4 hours
Safety evidence integration	Full SES with product-level and decision-level evidence classes; context-bound decision state records for high-impact decisions	SES manifests; decision state records	Safety evidence replay capability for sampled decisions
Dispensation gate maturity	All 7 gates (G1–G7) operational with automated evaluation	Gate completion records for all dispensation events	100% of dispensation events have complete gate results

Phase 2 → Phase 3 Transition Criteria:

Criterion	Minimum Threshold	Evidence
Reconciliation operational	All scheduled reconciliation types executing on cadence; break lifecycle operational	Reconciliation execution log; break inventory (may have open breaks)
Correction discipline proven	≥10 corrections processed through EP Delta discipline with non-destructive preservation	EP Delta samples; version lineage demonstrations
Supersession chains functional	Supersession chain management operational for authorizations	Supersession chain samples; canonical state determination demonstrations
Preservation bundles tested	At least 2 preservation bundles generated (live incident or exercise)	PB samples with completeness verification
Governance maturity	Change control operational; at least 1 recertification cycle completed	Change control records; recertification report
Governance approval	Governance body approves Phase 3 buildout	Governance approval record

AB.6 Advanced Institutionalization and Cross-Domain Readiness (Phase 4)

Phase 4 addresses capabilities that require mature underlying controls: cross-domain portability, conflict-of-process handling, resilience under stress, mature offboarding, and optional financial workflow integration.

Phase 4 Advanced Institutionalization Matrix:

Capability	Phase 4 Addition	Dependency	When to Adopt
Cross-domain portability	Evidence transfer between institutions or jurisdictions per Appendix Y; equivalence assessment; destination rebinding	Phase 3 reviewer readiness (evidence must be reviewer-safe before it is portable)	When institution participates in multi-entity or multi-jurisdiction workflows
Conflict-of-process handling	COP taxonomy (Appendix Y, Y.4); format/standard/authority/retention/disclosure conflict resolution	Phase 3 (requires mature evidence generation and bounded review)	When institution receives foreign-origin products or cross-border authorizations
Resilience and degraded modes	Degraded mode logic (Appendix Z); backpressure management; evidence continuity under stress	Phase 2 (requires reconciliation and break management as baseline)	When institution operates at scale or in critical-care settings
Mature offboarding	Full offboarding proof bundle (Appendix I); final reconciliation; open breaks disclosure; legacy transition manifest	Phase 3 (requires reviewer-ready evidence and preservation bundles)	Before any system transition, pilot conclusion, or participant exit
Optional financial workflows	Section 12 controls; Appendix W claim gates; temporal assessment; adjustment/reversal discipline	Phase 3 (requires mature authorization, custody, and safety evidence)	Only when claim/reimbursement evidence linkage is in institutional scope
Adversarial failure detection	Appendix U adversarial patterns; detection logic; containment for intentional abuse	Phase 2 (requires reconciliation and basic incident response)	When institution faces elevated counterfeit, diversion, or fraud risk
Advanced state governance	Full canonical state management (Appendix V); conflict resolution; parallel-state handling	Phase 3 (requires supersession chains and reviewer replay)	When institution manages complex authorization or product state environments

Phase 4 is not a prerequisite for operational benefit. Phases 1–3 produce substantial, standalone value. Phase 4 capabilities are adopted when the institution's operational context requires them — not as a mandatory destination.

AB.7 Dependency and Sequencing Logic

Dependency and Sequencing Matrix:

Capability	Depends On	Must Precede	Invalid Without
CPO registration	Nothing (foundational)	All provenance, authenticity, and custody controls	Product identity — framework cannot operate without CPO
Basic provenance	CPO	Multi-node provenance; reconciliation	Product reference anchor
AES generation	Nothing (foundational)	Dispensation gates; supersession chains	Authorization evidence — dispensation cannot be verified
Custody event logging	CPO (product reference)	Reconciliation; full chain replay; dispensation gates	Product identity for custody event linkage
Hold-only containment	Custody event logging (to identify what to hold)	Break management; recall workflows	Evidence of what is held and why
Content-addressed storage	Nothing (infrastructure)	All evidence integrity verification; preservation bundles	Tamper detection — evidence integrity unverifiable
Reconciliation	Phase 1 evidence (PAES, AES, CES)	Break management; correction discipline	Evidence artifacts to reconcile
EP Delta discipline	Content-addressed storage; governance approval chain	Supersession chains; correction workflows	Non-destructive preservation — corrections destroy prior state
Preservation bundles	Content-addressed storage; break management	Legal hold; incident investigation; offboarding	Evidence collection for incidents
Tiered reviewer access	Evidence generation (something to access)	Minimal disclosure profiles; PARP	Evidence — access controls without evidence are vacuous
Dispensation gates (full G1–G7)	PAES, AES, CES, SES all operational	Reviewer-ready dispensation verification	Upstream evidence sets — gates cannot evaluate absent evidence
Claim evidence linkage	Dispensation gates; PAES, AES, CES, SES	Claim gates (CG-1–CG-6); temporal assessment	Upstream evidence chain — claims cannot be evidence-linked without it
Cross-domain portability	Phase 3 reviewer readiness	Nothing (terminal capability)	Reviewer-safe evidence — non-reviewable evidence is not safely portable

Invalid Adoption Shortcuts (High-Risk):

Shortcut	Risk	Why It Fails
Claim processing before custody evidence	Claims approved without custody chain verification	BRK-FIN-001: claims without dispensation evidence; undetectable

Shortcut	Risk	Why It Fails
		diversion
Automated gates before evidence generation	Gates evaluate absent or unreliable evidence	False PASS results; dispensation proceeds on unverified states
Correction before preservation	Corrections overwrite prior states	Lost audit trail; silent overwrites (LT-07); governance violation
Portability before bounded review	Foreign evidence imported without disclosure controls	Over-disclosure; privacy violation; uncontrolled data export
Full scale before governance	High-volume operations without approval chains or change control	Ungoverned exceptions; accountability gaps; incident paralysis

AB.8 Phase Transition Gates and Approval Criteria

Phase Transition Gate Matrix:

Transition	Gate Criteria	Evidence Required	Blocking Conditions	Approval Authority
Entry → Phase 1	Institutional decision to adopt; governance sponsor identified; infrastructure for content-addressed storage available	Governance sponsor designation; infrastructure readiness assessment	None — any institution can begin Phase 1	Institutional leadership
Phase 1 → Phase 2	Phase 1 controls generating evidence consistently; hold-only tested; preservation baseline met; governance minimum established	Per AB.4 transition criteria table	Unresolved evidence generation gaps >5% of events; no hold-only test; governance structure absent	Governance body (or sponsor if governance body not yet formed)
Phase 2 → Phase 3	Reconciliation operational; correction discipline proven; supersession functional; preservation bundles tested; change control active	Per AB.5 transition criteria table	Reconciliation not executing on cadence; no EP Delta evidence; no preservation bundle generated	Governance body
Phase 3 → Phase 4	Full reviewer readiness; all dispensation gates operational; checks pack executable; query pack adapted; retrieval SLOs met	Phase 3 readiness indicators per AB.5 matrix	Checks pack <90% executable; query pack not adapted; retrieval SLO not met; PARP discipline not operational	Governance body with examiner readiness attestation

Rollback and Pause Conditions:

Condition	Response
Evidence generation rate drops below threshold during phase expansion	Pause expansion; investigate root cause; remediate before proceeding
SEV-1 break detected attributable to phase	Pause transition; containment per Appendix C;

Condition	Response
transition activity	investigate; governance review before resuming
Governance body determines phase expansion is premature	Pause or rollback to prior phase; document rationale; define remediation conditions
Integrity failure (BRK-INTEG) detected in newly implemented control	Immediately contain affected scope; investigate; restore valid state before proceeding

AB.9 Minimal Roles, RACI, and Governance-by-Phase

Minimal Roles and RACI-by-Phase Matrix:

Role	Phase 1	Phase 2	Phase 3	Phase 4
Governance sponsor	Required — individual champion with authority to approve holds and corrections	Required — may evolve into governance body chair	Governance body operational; sponsor role transitions to strategic oversight	Mature governance body with full committee structure
Evidence operator	Required — staff generating PAES, AES, custody ILS	Expanded — reconciliation execution; break management	Expanded — SES generation; decision state records; evidence retrieval	Expanded — portability; resilience; financial workflow evidence
Custody logger	Required — logs CUS_RECEIPT, CUS_DISPENSATION, CUS_HOLD	Expanded — full event taxonomy; storage conditions; excursions	Maintained	Maintained
Approval authority (holds/corrections)	Required — dual authorization for holds and corrections	Expanded — break containment approval; change control participation	Expanded — Tier 2 access approval; PARP review; recertification	Full RACI per Appendix G
Reviewer support	Minimal — responds to basic queries	Expanded — break investigation support; reconciliation report production	Full examiner support function — evidence retrieval; query pack execution; PARP administration	Cross-domain review support; portability evidence coordination
Quality / safety function	Not required in Phase 1 (but beneficial)	Recommended — excursion assessment; safety alert review	Required — SES generation; decision state governance; safety evidence refresh	Required — adversarial pattern detection; resilience monitoring

Phase 1 Minimum Governance Structure:

- One governance sponsor with dual-authorization partner for holds and corrections.
- Documented RACI for: product registration, custody logging, hold placement, hold release, correction approval, evidence preservation.

- No formal governance committee required in Phase 1 — committee structure deferred to Phase 2.

AB.10 Common Adoption Failure Modes and Mitigations

Adoption Failure Mode and Mitigation Matrix:

Failure Mode	Description	Risk	Mitigation
Scope overload	Attempting to implement all controls simultaneously	Implementation paralysis; no benefit delivered	Follow phased adoption; begin with Phase 1 minimum viable set
Automation before evidence	Automating dispensation gates before evidence artifacts are reliably generated	False PASS/FAIL results; unverified dispensation	Phase 1: generate evidence manually or semi-automatically; automate gates only in Phase 2–3
Weak custody before financial	Integrating claim/reimbursement workflows before custody chain evidence is reliable	Claims approved without custody verification; financial exposure	Defer financial workflows to Phase 4; require Phase 3 custody maturity
Broad disclosure before bounded review	Expanding evidence access without tiered access, purpose limitation, or PARP	Privacy violation; surveillance creep; regulatory exposure	Implement bounded review discipline (Phase 3) before expanding access scope
No preservation before correction	Implementing correction capability without non-destructive EP Delta discipline	Silent overwrites; lost audit trails; LT-07 violations	Implement content-addressed storage and EP Delta discipline in Phase 2 before enabling corrections
No phase-exit criteria	Moving to next phase without verifying prior phase maturity	Accumulated gaps; fragile architecture; hidden governance debt	Enforce phase transition gates (AB.8) with documented evidence
Portability too early	Attempting cross-border or cross-institution evidence transfer before reviewer readiness	Non-reviewable evidence exported; disclosure conflicts; integrity gaps	Defer portability to Phase 4; require Phase 3 reviewer readiness
Big-bang migration	Replacing all legacy systems simultaneously instead of layering framework controls	Operational disruption; data loss; rollback difficulty	Additive layering; framework operates alongside legacy; offboarding-ready from Phase 1

AB.11 Worked Adoption Patterns

Worked Adoption Pattern Table:

Pattern	Starting Point	Phase 1 Focus	Phase 2 Focus	Phase 3 Focus	Phase 4 (If Applicable)
Hospital	SP-PART	CPO	Full custody event	SES integration	Optional: claim

Pattern	Starting Point	Phase 1 Focus	Phase 2 Focus	Phase 3 Focus	Phase 4 (If Applicable)
pharmacy group	(electronic prescribing exists; barcode scanning at receipt)	registration; AES generation leveraging existing e-prescribing; custody logging at dispensing cabinets; basic hold-only	taxonomy; reconciliation (authorization-dispensation alignment); EP Delta discipline for prescription corrections	with existing CDSS; decision state records for overrides; full dispensation gates; examiner query pack	evidence linkage to existing billing system
Regional distributor	SP-LOW (paper-based shipping records; no content addressing)	CPO verification at receipt; basic provenance (manufacturer → distributor); custody logging for receipt and handoff; content-addressed storage	Multi-node provenance chain (manufacturer → distributor → customers); storage condition monitoring; excursion management; reconciliation	Reviewer-safe outputs for product integrity queries; full checks pack for provenance and custody; examiner retrieval SLOs	Cross-domain portability for multi-jurisdiction distribution
Multi-site health system	SP-FRAG (strong individual site systems; no cross-site evidence linkage)	Unified CPO registry across sites; standardized AES format; custody logging harmonized across sites	Cross-site reconciliation; break management across sites; supersession chain management for prescriptions spanning sites	Unified reviewer access across sites; standardized query pack; centralized PARP administration	Cross-domain portability between sites and external partners; resilience / degraded mode governance
Specialty pharmacy with claims	SP-FIN (claims system operational; upstream evidence weak)	Product authenticity at receipt; authorization verification; custody logging	Full custody chain; safety evidence integration; dispensation gates	Reviewer-ready evidence for claim support; temporal assessment capability	Claim evidence gates (CG-1–CG-6); temporal assessment; adjustment/reversal discipline

---

AB.12 Reader Action Map

Reader Action Map:

Starting State	Phase 1 Priority	Next Control Layer	Transition Gate	Expected Benefit
SP-LOW (low structure)	CPO + basic provenance + AES + custody logging + hold-only + content-addressed storage	Reconciliation + EP Delta + preservation	Phase 1 controls generating evidence ≥95%; hold tested; governance sponsor active	Counterfeit detection; authorization verification; basic audit trail
SP-PART (partial digital)	Gap-fill: add content addressing to existing digital records; add AES where missing; add hold-only	Full custody taxonomy + reconciliation + break management	Same as above, accelerated	Upgrade from tracking to evidence; break detection; proportional containment
SP-FRAG (fragmented)	Unify CPO across domains; standardize evidence format; harmonize custody logging	Cross-domain reconciliation + supersession + state determination	Reconciliation executing; corrections via EP Delta proven	Cross-domain consistency; unified break detection; version control
SP-BREV (good review, weak custody)	Custody event logging; provenance chain; storage conditions	Reconciliation + dispensation gates (leverage existing review infrastructure)	Custody chain operational; reconciliation running	Evidence-backed review (not just access-controlled review); custody integrity
SP-FIN (claims-focused)	Upstream evidence: product + authorization + custody + safety	Dispensation gates + reviewer readiness + temporal assessment	Phase 3 reviewer readiness met; upstream evidence mature	Evidence-linked claims; dispute-resilient payout; examiner-ready claim audit

Appendix AC — Control Mapping, Readiness Scoring, and Self-Assessment Pack for Product Authenticity, Authorization, Custody, Proof-of-Safety, and Bounded Review Workflows

AC.0 Purpose and Reader Orientation

> *"A credible operating framework requires more than declared controls. Institutions must be able to map control domains, assess evidence sufficiency, score readiness in a structured way, identify material gaps, and distinguish partial digitalization from reviewer-ready, replay-capable, and governably correctable operation."*

This appendix provides a structured self-assessment pack. It allows institutions to inventory their controls, score readiness across dimensions, identify and prioritize gaps, and determine whether they are prepared for examiner scrutiny, phase transitions, or advanced capabilities.

> *"The purpose of readiness scoring is not to compress complex architecture into a single number. It is to create a structured, evidence-backed view of which capabilities are present, which are immature, which are absent, and which gaps materially impair authenticity, authorization, custody, proof-of-safety, bounded verification, or correction readiness."*

What this appendix is: An operational self-assessment pack grounded in evidence, control sufficiency, replayability, and reviewer readiness.

What this appendix is not: A certification standard, legal compliance opinion, formal accreditation framework, or simplistic maturity model without evidence expectations.

AC.1 Control Domain Taxonomy

Control Domain Taxonomy Table:

Domain ID	Domain Name	Framework Sections	Key Artifacts
CD-01	Product authenticity	Sections 3.1, 4	CPO, PAES
CD-02	Provenance integrity	Sections 3.2, 4.2–4.6	Provenance manifest, hash-chained events
CD-03	Authorization / issuer legitimacy	Sections 3.3, 5.1–5.5	AES, issuer credential reference
CD-04	Prescription / instruction validity	Sections 3.4, 5.4	Prescription records, supersession chains
CD-05	Chain-of-custody	Sections 3.5, 6	CES, custody event chain, storage logs
CD-06	Dispensation / release integrity	Sections 3.6, 6.4	DEP-H, gate completion records
CD-07	Proof-of-safety evidence	Sections 3.7, 7	SES, decision state records
CD-08	Recall / quarantine /	Sections 3.8, 3.9, 8	Recall records, EP Deltas, hold-set

Domain ID	Domain Name	Framework Sections	Key Artifacts
	correction		records
CD-09	Bounded reviewer outputs	Sections 10, Appendix X	Tiered access records, PARP, query results
CD-10	Replay and reconstruction	Section 9.9, Appendix E	Replay execution records
CD-11	Governance and approval controls	Section 11	RACI, change control, recertification records
CD-12	Offboarding and portability	Section 13, Appendix I, Y	Offboarding proof bundle, portability records
CD-13	Financial workflows (optional)	Section 12, Appendix W	CLM-EP, claim gate results, temporal assessment

---

AC.2 Readiness Dimension Framework

Readiness is multi-dimensional. A control domain may be present but not evidence-backed, or evidence-backed but not replayable, or replayable but not reviewer-ready. The following dimensions capture this complexity.

Readiness Dimension Matrix:

Dimension ID	Dimension Name	Definition	Assessment Question
RD-01	Control existence	Is the control implemented and operational?	"Does this control execute in the operational environment?"
RD-02	Evidence sufficiency	Does the control produce content-addressed, integrity-verified evidence artifacts?	"Can I retrieve a content-addressed artifact proving this control executed?"
RD-03	Replayability	Can the control's execution and outcome be reconstructed at a historical point?	"Can I replay what happened on [date] for [subject] from stored evidence?"
RD-04	Governance sufficiency	Is the control governed by documented approval chains, RACI, and change control?	"Who approved this action, under what authority, and is that approval documented?"
RD-05	Reviewer readiness	Can an examiner independently verify this control through bounded access with purpose limitation and TTL?	"Can an examiner verify this control within 48 hours using standardized queries?"
RD-06	Bounded disclosure maturity	Does evidence access follow tiered access with pseudonymization, minimization, and post-access review?	"Is evidence disclosed at the minimum level necessary for the documented purpose?"
RD-07	Correction maturity	Are corrections processed through EP Delta discipline with non-destructive preservation?	"Is the prior state preserved when a correction is applied?"
RD-08	Portability	Can evidence be transferred to	"Can this evidence be exported

Dimension ID	Dimension Name	Definition	Assessment Question
	readiness	another system or jurisdiction with integrity preservation and documented handoff?	with content-addressed integrity to a receiving system?"
RD-09	Resilience maturity	Does the control operate under degraded conditions with evidence continuity?	"What happens to this control if [component] is unavailable for 4 hours?"

AC.3 Scoring Model and Maturity Bands

Scoring Model and Maturity Band Table:

Score	Band Label	Definition	Operational Indicator
0	Absent	Control not implemented; no evidence generated; no governance	No artifact, no process, no documentation
1	Ad hoc / fragmented	Control exists informally or inconsistently; evidence is paper-based or non-standardized; no content addressing	Some activity occurs but evidence is non-replayable, non-verifiable, and inconsistently produced
2	Partial / non-replayable	Control implemented with digital records but without content-addressed integrity, consistent logging, or reconciliation	Digital records exist but cannot be independently verified; no hash chain; no reconciliation
3	Controlled but limited	Control produces content-addressed evidence; basic reconciliation operational; governance documented; but limited replay capability and limited reviewer access discipline	Evidence artifacts retrievable and integrity-verifiable; reconciliation detects breaks; but examiner cannot independently replay or perform bounded verification
4	Reviewer-ready	Full evidence production with content addressing; reconciliation on cadence; EP Delta discipline; tiered reviewer access with purpose limitation; checks pack executable; query results reliable	Examiner can independently verify operational states; replay historical states; verify corrections were non-destructive; access evidence within SLO
5	Mature / scalable / portable	All Score 4 capabilities plus: cross-domain portability; resilience under stress; adversarial pattern detection; offboarding proof bundles; optional financial workflow integration	Evidence portable across jurisdictions or institutions; system operates under degraded conditions; offboarding can be completed without evidence loss

Scoring Conventions:

- Scores are assigned per control domain (CD-01 through CD-13) per readiness dimension (RD-01 through RD-09).
- A domain's overall score is the minimum across its critical dimensions (not the average) — a domain with Score 4 evidence sufficiency but Score 1 governance sufficiency is governed by its weakest critical dimension.

- Critical dimensions vary by domain; the self-assessment questionnaire (AC.6) identifies which dimensions are critical for each domain.

AC.4 Evidence Expectations by Score

Evidence Expectations by Score Matrix:

Score	Evidence Artifacts Expected	Governance Visible	Replay Capable	Reviewer Output
0	None	None	No	None
1	Paper records, screenshots, or ad-hoc digital files; no standardized format; no integrity markers	Informal approvals (email, verbal)	No (evidence not structured for replay)	Raw documents only; no standardized query capability
2	Digital records in databases or files; structured fields; but no content addressing; no hash chaining	Documented procedures exist; approval records in system	Partial (records can be queried but integrity not independently verifiable)	System-generated reports; not examiner-standardized
3	Content-addressed artifacts (ILS, manifests); hash-chained event sequences; reconciliation reports; EP Deltas for corrections	RACI documented; approval chains in content-addressed records; change control active	Yes for most operational states; some gaps in historical reconstruction	Basic query-safe views; Tier 0 aggregate reports; limited Tier 1
4	Full evidence packs per Appendix B templates; preservation bundles per Appendix F; all corrections via EP Delta; checks pack executable	Full governance per Appendix G RACI; recertification current; material change triggers documented	Full replay per Section 9.9 requirements; all replay types functional	Full tiered access; minimal disclosure profiles; PARP operational; examiner queries within SLO
5	All Score 4 plus: cross-domain portability evidence; equivalence assessments; offboarding proof bundles; resilience evidence; optional CLM-EP	Score 4 plus: cross-domain governance; conflict-of-process handling; adversarial pattern governance	Score 4 plus: replay under stress conditions; cross-domain replay	Score 4 plus: cross-domain reviewer access; VOP capability; cross-border query handling

---

AC.5 Gap Taxonomy and Materiality

Gap Taxonomy and Materiality Table:

Gap Class	Code	Definition	Materiality	Impact
Absent control	GAP-ABS	Control not implemented in any form	Blocking (if in Phase 1 minimum set); Material (if in current target phase)	Cannot advance to next phase; operational state unverifiable for this domain
Undocumented control	GAP-UNDOC	Control exists operationally but lacks evidence documentation	Material	Examiner cannot verify; replay not possible; governance unverifiable
Weak evidence	GAP-WKEV	Evidence generated but not content-addressed, not integrity-verified, or not consistently produced	Material	Evidence may be disputed; tamper detection absent; reconciliation unreliable
Insufficient replayability	GAP-RPLY	Evidence exists but historical state reconstruction is not possible (missing version lineage, missing EP Deltas, missing preservation)	Material for reviewer readiness	Examiner cannot replay; dispute resolution impaired; adverse event investigation limited
Stale state dependence	GAP-STALE	Operations proceed on evidence or credentials beyond applicable freshness window without re-verification	Material	Expired evidence may not reflect current conditions; stale authorization may be invalid
Broad disclosure without bounded review	GAP-DISC	Evidence accessible without tiered access controls, purpose limitation, or TTL	Material (privacy/compliance risk)	Over-disclosure; privacy violation; surveillance creep
Correction without preservation	GAP-CORR	Corrections applied by overwriting prior state; no EP Delta; no version lineage	Blocking (governance violation)	Lost audit trail; LT-07 violation; examiner cannot verify correction history
Portability without continuity	GAP-PORT	Evidence exported without integrity verification, format documentation, or equivalence assessment	Material (for cross-domain operations)	Imported evidence unreliable; integrity unverifiable at destination
Financial progression without evidence	GAP-FIN	Claims approved or paid without evidence linkage to upstream product, authorization, custody, or safety states	Blocking (for financial workflows)	Claims proceed on unverified states; financial exposure; dispute vulnerability

Materiality Classification:

Classification	Definition	Phase Impact
Blocking	Gap prevents advancement to target phase or creates governance violation	Must be remediated before phase transition
Material	Gap significantly impairs a control domain but does not prevent all operations	Should be remediated within current phase; documented with risk acceptance if deferred
Minor	Gap affects efficiency or completeness but does not impair core control integrity	Remediated per improvement cycle; documented

---

AC.6 Self-Assessment Questionnaire Pack

Self-Assessment Questionnaire Matrix (Representative — by Domain):

CD-01: Product Authenticity:

Question	Positive Evidence	Weak Answer Indicator	Follow-Up
Are all products registered with a Canonical Product Object (CPO) before entering the custody chain?	CPO registry with content-addressed records; 100% coverage for products in scope	"Most products are registered" — implies coverage gaps	Quantify coverage percentage; identify unregistered product categories
Is manufacturer identity verified through credential evidence (not assertion alone)?	AES with manufacturer credential reference, revocation check, and freshness status	"We trust our suppliers" — no evidence-backed verification	Implement AES generation with credential verification at receipt
Can product authenticity be verified at any point by hash chain traversal?	Provenance manifest with PASS integrity verification for sampled products	"We have serial numbers" — serial numbers alone are not content-addressed evidence	Assess whether serial numbers are linked to content-addressed provenance chain

CD-05: Chain-of-Custody:

Question	Positive Evidence	Weak Answer Indicator	Follow-Up
Are all custody transitions logged as ILS records with content-addressed integrity?	CES with hash-chained custody events; CUS_RECEIPT and CUS_DISPENSATION logged for all transactions	"We have receiving logs" — may be paper or non-content-addressed	Assess whether logs are digital, content-addressed, and hash-chained
Are storage conditions continuously monitored for condition-sensitive products?	Storage condition logs with excursion detection records	"We check temperatures daily" — periodic check vs. continuous monitoring	Assess monitoring granularity vs. product sensitivity requirements
Can the complete	Custody chain replay	"We can look up where	Test historical

Question	Positive Evidence	Weak Answer Indicator	Follow-Up
custody chain be replayed for any product unit?	demonstration for sampled products	things are" — current state query vs. historical replay	replay capability for sampled products

CD-09: Bounded Reviewer Outputs:

Question	Positive Evidence	Weak Answer Indicator	Follow-Up
Is reviewer access governed by tiered access (Tier 0/1/2) with documented purpose codes?	Access event records with tier, purpose code, and TTL; configuration documentation for access tiers	"Reviewers can access the system" — no tiered access; no purpose limitation	Implement tiered access controls before expanding reviewer access
Are Tier 2 access events subject to dual-control approval and PARP?	Tier 2 access records with dual-control approval; completed PARP within SLA	"We log who accesses what" — logging without governance is not bounded review	Implement PARP discipline and dual-control for Tier 2
Can examiner queries be answered within retrieval SLOs using standardized query packs?	Query execution demonstrations within SLO; results in standardized format	"We can pull reports" — ad hoc reporting vs. standardized examiner queries	Adapt Appendix E query pack to institutional retrieval infrastructure

---

AC.7 Readiness Scoring Worksheets

Readiness Scoring Worksheet Template — Product Authenticity and Provenance (CD-01, CD-02):

Dimension	Score (0–5)	Evidence Cited	Gap Identified	Gap Materiality
RD-01: Control existence	___	___	___	___
RD-02: Evidence sufficiency	___	___	___	___
RD-03: Replayability	___	___	___	___
RD-04: Governance sufficiency	___	___	___	___
RD-05: Reviewer readiness	___	___	___	___
RD-07: Correction maturity	___	___	___	___
Domain minimum score	___			

Repeat for each domain (CD-03 through CD-13). Critical dimensions vary by domain:

Critical Dimensions by Domain:

Domain	Critical Dimensions (Minimum Score Governs)
CD-01 Product authenticity	RD-01, RD-02, RD-03
CD-02 Provenance	RD-01, RD-02, RD-03
CD-03 Authorization	RD-01, RD-02, RD-04
CD-04 Prescription validity	RD-01, RD-02, RD-07
CD-05 Custody	RD-01, RD-02, RD-03
CD-06 Dispensation	RD-01, RD-02, RD-04

Domain	Critical Dimensions (Minimum Score Governs)
CD-07 Safety evidence	RD-01, RD-02, RD-03, RD-05
CD-08 Recall / correction	RD-01, RD-04, RD-07
CD-09 Bounded review	RD-01, RD-05, RD-06
CD-10 Replay	RD-03 (primary)
CD-11 Governance	RD-04 (primary)
CD-12 Offboarding / portability	RD-08
CD-13 Financial workflows	RD-01, RD-02, RD-04

AC.8 Gap Prioritization and Remediation Logic

Gap Prioritization Matrix:

Priority	Gap Characteristics	Remediation Timing	Examples
P1: Blocking	Gap prevents phase advancement or creates active governance violation	Immediate remediation before any expansion	GAP-CORR (correction without preservation); GAP-ABS for Phase 1 controls; GAP-FIN if financial workflows active
P2: Reviewer-facing	Gap will be visible to examiner; impairs reviewer confidence or evidence production	Remediate within current phase before examiner engagement	GAP-UNDOC; GAP-WKEV in domains subject to examination; GAP-RPLY for domains with active queries
P3: Replayability	Gap impairs historical reconstruction but does not block current operations	Remediate within current phase; acceptable to document and schedule	GAP-RPLY for non-critical domains; GAP-STALE for low-risk categories
P4: Governance	Gap in governance documentation or process maturity; controls operate but governance evidence is weak	Remediate at next recertification cycle	GAP-UNDOC for governance structures; missing RACI for non-critical activities
P5: Portability / resilience	Gap affects cross-domain or stress-condition capability; relevant only at Phase 4	Defer to Phase 4 planning; document in roadmap	GAP-PORT; resilience gaps; adversarial detection gaps

AC.9 Reviewer / Examiner Readiness Interpretation

Reviewer / Examiner Readiness Interpretation Matrix:

Readiness Level	Minimum Domain Scores	Capability	Limitation
Not reviewer-ready	Any critical domain below Score 2	No standardized examiner interaction possible	Examiner must rely on ad hoc evidence and institutional representation
Triage-only ready	All critical domains at Score 2; some at	Basic examiner queries answerable with	Examiner cannot independently verify;

Readiness Level	Minimum Domain Scores	Capability	Limitation
	Score 3	institutional assistance; not independently verifiable	replay not available; limited bounded access
Bounded-review-capable	All critical domains at Score 3; CD-09 (bounded review) at Score 3+	Examiner can access evidence through basic tiered access; content-addressed artifacts verifiable	Limited replay; limited PARP discipline; examiner may need operational support for complex queries
Replay-capable	All critical domains at Score 4; CD-10 (replay) at Score 4	Examiner can independently replay historical states; full checks pack executable	May lack cross-domain portability or resilience under stress
Offboarding-capable	All critical domains at Score 4; CD-12 (offboarding) at Score 4	Institution can execute offboarding with full proof bundle; legacy transition with integrity preservation	May lack advanced portability or financial workflow integration
Advanced / portable	All domains at Score 4+; relevant domains at Score 5	Cross-domain evidence portability; resilience under stress; full adversarial detection; optional financial integration	Represents target state; continuous improvement continues

AC.10 Worked Example Assessments

Worked Example Assessment Table:

Institution	Profile	Score Summary	Key Gaps	Remediation Priority	Likely Next Phase
Community pharmacy group (SP-PART)	Electronic prescribing; barcode scanning; no content addressing; paper custody logs	CD-01: 2, CD-03: 2, CD-05: 1, CD-06: 1, CD-09: 0	GAP-WKEV (CD-01, CD-03: digital but not content-addressed); GAP-ABS (CD-05: no digital custody logging); GAP-ABS (CD-09: no bounded review)	P1: Implement custody logging (CD-05); P2: Add content addressing to existing records (CD-01, CD-03); P3: Plan bounded review	Phase 1 (gap-fill for custody and content addressing)
Regional distributor (SP-LOW)	Paper shipping records; no digital evidence; no formal governance	CD-01: 0, CD-02: 0, CD-05: 0, CD-11: 0	GAP-ABS across CD-01, CD-02, CD-05, CD-11	P1: Full Phase 1 implementation — CPO, provenance, custody, hold-only, governance	Phase 1 (full)
Hospital	Strong	CD-01: 3,	GAP-PORT (cross-	P2: Cross-site	Phase 2–3

Institution	Profile	Score Summary	Key Gaps	Remediation Priority	Likely Next Phase
system (SP-FRAG)	pharmacy systems; CDSS operational; good access controls; weak cross-site linkage	CD-03: 3, CD-05: 3, CD-07: 3, CD-09: 3, cross-site: 1	site evidence not linked); GAP-RPLY (cross-site replay not possible)	evidence linkage; unified reconciliation; P3: Standardize reviewer access across sites	(site unification)
Specialty pharmacy with claims (SP-FIN)	Claims system mature; upstream evidence weak; no temporal assessment	CD-01: 2, CD-05: 2, CD-06: 1, CD-13: 2 (claims operational but not evidence-linked)	GAP-FIN (claims without upstream evidence); GAP-WKEV (upstream domains not content-addressed)	P1: Upstream evidence (product, authorization, custody, safety); P2: Evidence-linked claim gates	Phase 1 (upstream), then Phase 4 (financial integration)

AC.11 Summary Scorecard and Action Map

Summary Scorecard and Action Map:

Domain	Score	Evidence Sufficiency	Material Gap	Remediation Priority	Readiness Implication
CD-01 Product authenticity	___ /5	Sufficient / Partial / Absent	___ (gap code)	P1 / P2 / P3 / P4 / P5	Blocks: Phase transition if <3 for target phase
CD-02 Provenance	___ /5	___	___	___	___
CD-03 Authorization	___ /5	___	___	___	___
CD-04 Prescription validity	___ /5	___	___	___	___
CD-05 Custody	___ /5	___	___	___	___
CD-06 Dispensation	___ /5	___	___	___	___
CD-07 Safety evidence	___ /5	___	___	___	___
CD-08 Recall / correction	___ /5	___	___	___	___
CD-09 Bounded review	___ /5	___	___	___	___
CD-10 Replay	___ /5	___	___	___	___
CD-11 Governance	___ /5	___	___	___	___
CD-12 Offboarding	___ /5	___	___	___	___

Domain	Score	Evidence Sufficiency	Material Gap	Remediation Priority	Readiness Implication
CD-13 Financial (optional)	___ /5	___	___	___	___

Scorecard Interpretation Rules:

- All critical domains at Score ≥3 → institution is minimally controlled (Phase 2 ready).
- All critical domains at Score ≥4 → institution is reviewer-ready (Phase 3 complete).
- Any critical domain at Score 0 or 1 → blocking gap; remediate before phase transition.
- Minimum domain score (lowest critical dimension within a domain) governs the domain score.
- Highest-priority remediation targets: domains with the largest gap between current score and target-phase requirement.

Action Logic:

```
For each domain:
  1. Assess current score per AC.7 worksheet
  2. Identify gaps per AC.5 taxonomy
  3. Classify materiality (blocking / material / minor)
  4. Prioritize per AC.8 matrix
  5. Map to remediation actions
  6. Verify readiness per AC.9 interpretation
  7. Document in scorecard
  8. Present to governance body for phase transition decision
```

References and Supporting Materials

---

1. ***Foundational Baseline Frameworks (Normative Anchors)*** *This implementation guidance acts as a cross-domain companion layer and relies on the structures, vocabularies, and governance models established in the following baselines:*

- **Baseline A: Ownership Integrity & Reconciliation Pack.** Provides the foundational architecture for Evidence Sets, reconciliation break taxonomies, hold-only containment logic, and non-destructive preservation disciplines (EP Deltas).
- **Baseline B: Operationalization & Conformance Track.** Defines the playbook structure, reference implementation profiles, RACI matrix conventions, change control governance, and tiered supervisory access models.
- **Baseline C: Operational Assurance Artifacts Addendum.** Specifies the Evidence Pack manifest templates, Immutable Log Segment (ILS) logging taxonomy, preservation bundle triggers, liability trigger catalogs, and redaction protocols.
- **Baseline D: Programmable Privacy & ZKP Framework.** Establishes the tiered disclosure ladder (Tier 0/1/2), proof-carrying compliance artifacts, Verifier Output Pack (VOP) conventions, TTL bounds, and freshness/revocation disciplines.
- **Baseline E (Optional): Payments & Settlement Constitution.** Provides the blueprint for evidence-linked settlement confirmation, payout gating, and the management of financially consequential workflows.

2. Cryptographic and Technical Standards

- **Secure Hash Algorithms:** SHA-256 (or equivalent cryptographic standards), utilized for generating content-addressed manifests, Canonical Product Objects (CPOs), and ensuring tamper-evident hash-chaining across all Immutable Log Segments (ILS).
- **Content-Addressed Storage Architecture:** Operational standards governing immutability by construction, ensuring that artifacts cannot be modified after storage without breaking the hash linkage.

3. Healthcare Alignment Objectives (Non-Normative Context)

Note: This framework provides an operational evidence layer and does not replace medical truth, institutional review, or regulatory decrees. The following represent contextual alignment objectives referenced to map operational evidence to real-world healthcare compliance:

- **Product Identification and Serialization:** Standards such as Global Trade Item Numbers (GTIN), National Drug Codes (NDC), or equivalent serialization identifiers used to anchor Canonical Product Objects (CPOs).
- **Good Distribution Practice (GDP) & Supply Chain Security:** Regulatory standards (analogous to the US DSCSA or EU FMD) that align with the framework's Product

Authenticity Evidence Set (PAES), Custody Evidence Set (CES), and chain-of-custody handoff workflows.

- **Pharmacovigilance and Safety Reporting:** Institutional and regulatory frameworks for capturing adverse events, monitoring contraindications, and executing product recalls, structurally supported by the Safety Evidence Set (SES) and Context-Bound Decision States.
- **Data Privacy and Minimization Requirements:** Institutional health data protection policies (e.g., HIPAA or GDPR alignment objectives) supported by the framework's tiered reviewer access and pseudonymization protocols.
