



CRYPTOGRAPHIC AUDIT & TRUST LEDGER

Sample Evidence Pack

Eleven ledger entries covering one mapping version from spreadsheet import to published, sealed record — with every hash computed from the payloads printed inside, so you can verify it yourself.

CHAIN HEAD

fb549d38c456c1a09f73f5f2d306fdec3e01419a7ef80171443f8a42daf02ac4

ENTRIES	ALGORITHM	WINDOW
11	SHA-256	2026-09-16 → 2026-09-17

What this pack is

All tenants, actors, schema names, identifiers, IP addresses, object keys, and KMS identifiers in this pack are **synthetic**. No real customer, patient, or production data is present. The cryptographic chain inside it is genuine: every hash was computed from the payloads printed in Section 03 and can be independently re-derived with the bundled verifier.

Scope of the record

TENANT	Northlake Health Plan (sample tenant)
SECTOR	health plan – claims interoperability
TENANT ULID	0000000000018DJRFAEBXG73OMK
MAPPING	core-claims-to-fhir-r4
MAPPING ULID	00000000000YC0000000000000000
SOURCE SCHEMA	Core Claims Extract 1.0.0
TARGET SCHEMA	FHIR R4 Coverage & Claim 1.0.0
COMPLIANCE REGIMES	hipaa, cfr_part_11, cmmc_l2
ENTRIES	11
WINDOW	2026-09-16T23:06:40.000Z → 2026-09-17T05:25:40.000Z
LEDGER SCHEMA	audit schema 1.1.0
PRODUCT VERSION	magellan-data 1.6.2

Chain parameters

These are the only facts you need to re-derive the entire record. Nothing here is secret, and nothing here is proprietary.

HASH ALGORITHM	sha256
ENTRY HASH	$\text{entry_hash} = \text{sha256}(\text{prev_hash} \parallel \text{payload_sha256})$
PAYLOAD HASH	$\text{payload_sha256} = \text{sha256}(\text{canonical}(\text{payload}))$
CHAIN FORMULA	$H(n) = \text{sha256}(H(n-1) \parallel \text{canonical}(\text{entry}_n))$
GENESIS PREV_HASH	0000000000000000000000000000000000000000000000000000000000000000
IDENTIFIER POLICY	ULID only – Crockford base32, 26 characters

CANONICALIZATION

JSON with object keys sorted lexicographically, no insignificant whitespace (separators ',' and ':'), UTF-8 encoding, no trailing newline. Hashes are hex-encoded; prev_hash and payload_sha256 are hashed as raw 32-byte values, not as hex text.

Why canonicalization is spelled out. A hash is only as trustworthy as the byte sequence that produced it. Two systems that agree on the formula but disagree on key order or whitespace will disagree on the hash — which looks exactly like tampering. The rule above is published so a verifier never has to guess.

What a prospect should ask for. Any vendor claiming an audit trail can produce a log. Ask instead: can I re-derive your hashes without your software running? If the answer is no, the trail is an assertion about the past, not evidence of it.

The record in plain terms

Read this page first. It is the same eleven entries that follow in Section 03, described without hashes — so you can check that a tamper-evident ledger is recording something a human would recognize.

	STAGE	WHAT HAPPENED	ENTRIES
1	Import	A claims field inventory spreadsheet is imported. That single action creates the source schema, the target schema, and a mapping at one shared version. From this point the three version independently.	#1–#3
2	Schemas approve first	Both pinned schema versions are reviewed and move to Approved & Published. This is a hard gate: a mapping version cannot enter approval until every schema version it pins has already been approved and published.	#4–#5
3	The engine advises, a person decides	The Semantic Match Engine proposes 38 links with confidence scores and the algorithm class behind each one. Nothing is written to the mapping without a named reviewer's decision.	6
4	Review, including the rejections	A named approver reviews all 164 links and rejects three — on unit and semantics grounds — with the reason recorded for each. The rejections are part of the permanent record, not discarded.	7
5	Release signature	The approver signs the mapping version for publication. The approver is not the contributor who drafted it, so the record shows separation of duties rather than asserting it.	8
6	Published and pinned	Mapping version 1.0.0 is published against source 1.0.0 and target 1.0.0. Any later run reproduces from those three pinned versions — including years from now, after both schemas have moved on.	9
7	Exported as evidence	An auditor exports the pack for an internal audit walkthrough, recording the chain head as it stood at export time.	10
8	Sealed to WORM storage	The chain head is flushed to Object Lock in compliance mode with seven-year retention. Retention cannot be shortened, including by the account root.	11

THE PART THAT IS HARD TO FAKE

Two facts in this record are uncomfortable to reproduce by hand. The *order* of the approvals is not a policy statement on a wiki — the mapping version's own entry carries a hash that only closes if both schema approvals precede it. And the three rejected suggestions are still in the ledger with their reasons, which means the record shows judgment being exercised rather than an engine being rubber-stamped.

The ledger, in full

Each entry prints its own canonical payload and all three hashes. Recompute any one of them and you get the value shown — or you don't, which is the point.

Entry #01 · SchemaIngested

2026-09-16T23:06:40.000Z

ENTRY ULID	O1M2P7HTOOXZWG4H29YN3PZ7AZ
ACTOR	A. Whitfield (000000000024H36H2NCSVRH68A)
ROLE AT TIME OF ACTION	CONTRIBUTOR
SUBJECT	schema_version 0000000000Y400000000000000 · version 1.0.0
REQUEST ID	req-6cd0ea581ab0
SOURCE IP	10.14.8.40
RATIONALE	Bulk import of the claims field inventory supplied by the data owner.

CANONICAL PAYLOAD (THE BYTES THAT WERE HASHED)

```
{
  "event": "spreadsheet_import",
  "import_batch_ulid": "01M2P7HT00WAJC0E5HF0DZ3HMP",
  "source_file": "core-claims-field-inventory.xlsx",
  "source_file_sha256": "43d1a9be4615ca7be07a81aaf492c64ec0931a380e2438e8b7f932ca0824c1cc",
  "sheets_read": 4,
  "columns_detected": 218,
  "schema_kind": "source",
  "schema_name": "Core Claims Extract",
  "schema_version": "1.0.0",
  "entities": 12,
  "attributes": 218,
  "shared_import_version": "0.1.0",
  "note": "Import created source schema, target schema, and mapping at one shared version; the three version independently from here."
}
```

PAYLOAD_SHA256

a6e0d569877cd2ff10fe9b3e7db2de25c87809802e55e253237abbf8afc10f05

PREV_HASH

0000000000000000000000000000000000000000000000000000000000000000

ENTRY_HASH

3dca562ce21a3b1f3ee9c06ad362dc39c7443ee89f6f4455a100f409e5f6e97a

ENTRY ULID	O1M2P7KMKOA5AJKEGVV84C5WP
ACTOR	A. Whitfield (000000000024H36H2NCSVRH68A)
ROLE AT TIME OF ACTION	CONTRIBUTOR
SUBJECT	schema_version 0000000000Y800000000000000 · version 1.0.0
REQUEST ID	req-7bb086aa0e97
SOURCE IP	10.14.8.41
RATIONALE	Target profile registered from the same import batch.

CANONICAL PAYLOAD (THE BYTES THAT WERE HASHED)

```
{
  "event": "spreadsheet_import",
  "source_file": "core-claims-field-inventory.xlsx",
  "schema_kind": "target",
  "schema_name": "FHIR R4 Coverage & Claim",
  "schema_version": "1.0.0",
  "profile_baseline": "HL7 FHIR R4 (v4.0.1)",
  "entities": 9,
  "attributes": 164,
  "shared_import_version": "0.1.0"
}
```

PAYLOAD_SHA256	49f09e4cff706078e72b8c3dad486116c1d8beae7f1e00072b6d3de4d1e8d745
PREV_HASH	3dca562ce21a3b1f3ee9c06ad362dc39c7443ee89f6f4455a100f409e5f6e97a
ENTRY_HASH	d5d99d915863768a38958f51a3d17714e3bbbb8a945aa9752dea6ed739ba09f1

ENTRY ULID	O1M2P7Q9SOGPAORTG6FPCVW8VO
ACTOR	A. Whitfield (000000000024H36H2NCSVRH68A)
ROLE AT TIME OF ACTION	CONTRIBUTOR
SUBJECT	mapping 0000000000YC00000000000000 · version O.1.0
REQUEST ID	req-162dd41cf1db
SOURCE IP	10.14.8.42
RATIONALE	Draft opened against the pinned schema versions registered at import.

CANONICAL PAYLOAD (THE BYTES THAT WERE HASHED)

```
{
  "mapping_name": "core-claims-to-fhir-r4",
  "pinned_source_schema_ulid": "0000000000Y400000000000000",
  "pinned_source_schema_version": "1.0.0",
  "pinned_target_schema_ulid": "0000000000Y800000000000000",
  "pinned_target_schema_version": "1.0.0",
  "draft_links": 164,
  "unresolved_links": 41
}
```

PAYLOAD_SHA256	4a780a4667ec7b48cf7580e9fa4861a1b022f2e4fb7f22b8c43444f9a67c84df
PREV_HASH	d5d99d915863768a38958f51a3d17714e3bbbb8a945aa9752dea6ed739ba09f1
ENTRY_HASH	5d33aa0026157d733213e2d0ff2aa3f18e63f2a3342b9633b548a7d0a90e1694

ENTRY ULID	O1M2PGOSWOW838CY6C4K3WMT5S
ACTOR	R. Okonkwo (0000000000QC0128HK8HAPCXW8)
ROLE AT TIME OF ACTION	APPROVER
SUBJECT	schema_version 0000000000Y400000000000000 · version 1.0.0
REQUEST ID	req-23614c5db8ee
SOURCE IP	10.14.8.43
RATIONALE	Source schema reviewed against the data-owner inventory. Approved and published before any mapping version referencing it could enter approval.

CANONICAL PAYLOAD (THE BYTES THAT WERE HASHED)

```
{
  "schema_name": "Core Claims Extract",
  "transition": "draft → approved_and_published",
  "reviewed_attributes": 218,
  "waived_checks": []
}
```

PAYLOAD_SHA256
dd61de2f06ef8682fc5cd73e9d6c13be15483e14d6ee24128f873355094dc29f

PREV_HASH
5d33aa0026157d733213e2d0ff2aa3f18e63f2a3342b9633b548a7d0a90e1694

ENTRY_HASH
49d40d8d267a13c640a384973d9e229eaf14b137a597f69c92ac53f36329a6c7

ENTRY ULID	O1M2PGMYDOEOBHFERRNPXQG98
ACTOR	R. Okonkwo (0000000000QC0128HK8HAPCXW8)
ROLE AT TIME OF ACTION	APPROVER
SUBJECT	schema_version 0000000000Y800000000000000 · version 1.0.0
REQUEST ID	req-7Ocea11b41df
SOURCE IP	10.14.8.44
RATIONALE	Target profile confirmed against FHIR R4 v4.0.1. Both pinned schema versions are now Approved & Published, so the mapping version may be submitted for approval.

CANONICAL PAYLOAD (THE BYTES THAT WERE HASHED)

```
{
  "schema_name": "FHIR R4 Coverage & Claim",
  "transition": "draft → approved_and_published",
  "reviewed_attributes": 164,
  "profile_baseline": "HL7 FHIR R4 (v4.0.1)",
  "waived_checks": []
}
```

PAYLOAD_SHA256

b3fdf160499e7473ec0ac091a031197c3323a4af6ff1b460acb4000022f8eb0b

PREV_HASH

49d40d8d267a13c640a384973d9e229eaf14b137a597f69c92ac53f36329a6c7

ENTRY_HASH

e6330973e6a0030f3dee8849c354595e170b062aaf361e8619aab902dfe6776a

ENTRY ULID	O1M2PJTGZORZST45IMDNBH5MRR
ACTOR	magellan-semantic-match (0000000000XRSM8NB6EY49J00H)
ROLE AT TIME OF ACTION	CONTRIBUTOR
SUBJECT	mapping 0000000000Y000000000000000 · version 0.1.0
MODEL	semantic-match@2.5
THRESHOLD PROFILE	claims-fhir-r4-v3
REQUEST ID	req-6b6738d8ea6e
SOURCE IP	10.14.8.45
RATIONALE	Semantic Match Engine proposals. Every suggestion was advisory: none was written to the mapping without a named reviewer's decision.

CANONICAL PAYLOAD (THE BYTES THAT WERE HASHED)

```
{
  "proposed_links": 38,
  "accepted_in_review": 35,
  "rejected_in_review": 3,
  "algorithm_classes": [
    "exact_match",
    "synonym",
    "hierarchy",
    "domain_equivalence",
    "ontology_equivalence",
    "pattern"
  ],
  "confidence_distribution": {
    "high": 22,
    "medium": 13,
    "low": 3
  },
  "pinned_source_schema_version": "1.0.0",
  "pinned_target_schema_version": "1.0.0",
  "sample": [
    {
      "source": "ClaimDetail.AdmitDate",
      "target": "Encounter.period.start",
      "confidence": 0.94,
      "class": "domain_equivalence"
    },
    {
      "source": "MemberRec.No",
      "target": "Patient.identifier[memberId].value",
      "confidence": 0.91,
      "class": "synonym"
    }
  ]
}
```

PAYLOAD_SHA256
75cb7d881190bae28e7a8bcd00404bcfb89349b8273f642f2d27a6465ecec46b

PREV_HASH
e6330973e6a0030f3dee8849c354595e170b062aaf361e8619aab902dfe6776a

ENTRY_HASH
573d28b047d0aca34e1a4891610eea971153924ddde8274a676e466f1f7772c8

ENTRY ULID	O1M2PRA9ZOH15OCFXM44RFJ9NC
ACTOR	R. Okonkwo (0000000000QC0128HK8HAPCXW8)
ROLE AT TIME OF ACTION	APPROVER
SUBJECT	mapping 0000000000YC00000000000000 · version O.1.0
REQUEST ID	req-368803ad11bc
SOURCE IP	10.14.8.46
RATIONALE	Line-by-line review. Three engine suggestions rejected on unit and semantics grounds; rejections are recorded with their reasons.

CANONICAL PAYLOAD (THE BYTES THAT WERE HASHED)

```
{
  "links_reviewed": 164,
  "links_accepted": 161,
  "links_rejected": 3,
  "rejections": [
    {
      "source": "ClaimDetail.BalanceAmt",
      "target": "Claim.total[adjudication].value",
      "reason": "Units differ: source is cents, target requires decimal units. Needs an explicit transform, not a rename."
    },
    {
      "source": "MemberRec.EligDt",
      "target": "Coverage.period.end",
      "reason": "Source is a snapshot date, not a coverage end date."
    },
    {
      "source": "ClaimDetail.ProcCnt",
      "target": "Claim.item.sequence",
      "reason": "Count is not a sequence number."
    }
  ],
  "pinned_source_schema_version": "1.0.0",
  "pinned_target_schema_version": "1.0.0"
}
```

PAYLOAD_SHA256
657bc97f6a6104038c8123eae3ff6b742bbe117deadc426aebaa77d6e74526b2

PREV_HASH
573d28b047d0aca34e1a4891610eea971153924ddde8274a676e466f1f7772c8

ENTRY_HASH
c85b69e3e6c745ece5b4553cb0a8850e0ae71ca10536bdbbfc0231647dc378854

ENTRY ULID	O1M2PS9E2OS8GSR66SNKVKD13N
ACTOR	R. Okonkwo (0000000000QC0128HK8HAPCXW8)
ROLE AT TIME OF ACTION	APPROVER
SUBJECT	mapping 0000000000YC00000000000000 · version O.1.0
REQUEST ID	req-cba083b770c2
SOURCE IP	10.14.8.47
RATIONALE	Named approver released the mapping version. The approver is not the contributor who drafted it.

CANONICAL PAYLOAD (THE BYTES THAT WERE HASHED)

```
{
  "signature_meaning": "approval of mapping version 0.1.0 for publication",
  "electronic_signature_basis": "21 CFR Part 11 11.100 / 11.200",
  "signed_mapping_version": "0.1.0",
  "pinned_source_schema_version": "1.0.0",
  "pinned_target_schema_version": "1.0.0",
  "approval_gate": "satisfied - both pinned schema versions Approved & Published",
  "manifest_sha256": "ed70d779250bc8fd34ba258bc718980482e491e984db84f57fe4fbeddee9eb24"
}
```

PAYLOAD_SHA256
4d16809c7325f3e72d20f2a89593f0bc5ce02bef7a5d16157f317f3abba287e6

PREV_HASH
c85b69e3e6c745ece5b4553cb0a8850e0ae71ca10536bdbfc0231647dc378854

ENTRY_HASH
8acdfca8db3b0b4689f8d074603b5b10cd32958386e1c8dbde1ade5ac566a3bc

ENTRY ULID	O1M2PSMDMO2TV9JAD3AKSQB7Y4
ACTOR	R. Okonkwo (0000000000QC0128HK8HAPCXW8)
ROLE AT TIME OF ACTION	APPROVER
SUBJECT	mapping 0000000000YC00000000000000 · version 1.0.0
REQUEST ID	req-fc491a474e7d
SOURCE IP	10.14.8.48
RATIONALE	Version 1.0.0 published and pinned. Any downstream run of this mapping reproduces from these three pinned versions.

CANONICAL PAYLOAD (THE BYTES THAT WERE HASHED)

```
{
  "mapping_name": "core-claims-to-fhir-r4",
  "transition": "approved → published",
  "published_version": "1.0.0",
  "pinned_source_schema_ulid": "0000000000Y400000000000000",
  "pinned_source_schema_version": "1.0.0",
  "pinned_target_schema_ulid": "0000000000Y800000000000000",
  "pinned_target_schema_version": "1.0.0",
  "active_links": 161,
  "transforms": 24
}
```

PAYLOAD_SHA256
cf39ca274b2467fd8ecd1b4bcb1e24e1792ce45808e05e5c597c746e9f7f7748

PREV_HASH
8acdfca8db3b0b4689f8d074603b5b10cd32958386e1c8dbde1ade5ac566a3bc

ENTRY_HASH
708a4c1f08295a4a004bff41d0cd61c7fe69743f25411893965a5e50afa34583

ENTRY ULID	O1M2PXOENOGESKY4XHG9ZHGQO
ACTOR	M. Delacroix (0000000000SG8J4CT4ANK7F24S)
ROLE AT TIME OF ACTION	AUDITOR
SUBJECT	mapping 0000000000YC00000000000000 · version 1.0.0
REQUEST ID	req-b31dec476039
SOURCE IP	10.14.8.49
RATIONALE	Evidence pack exported for an internal audit walkthrough. The pack is verifiable without runtime access to Magellan.

CANONICAL PAYLOAD (THE BYTES THAT WERE HASHED)

```
{
  "export_format": "evidence-pack/1",
  "regimes": [
    "hipaa",
    "cfr_part_11",
    "cmmc_l2"
  ],
  "control_citations": [
    "HIPAA 164.312(b)",
    "21 CFR Part 11 11.10(e)",
    "CMMC L2 3.3 AU-2/AU-3/AU-9/AU-11"
  ],
  "entries_covered": 9,
  "chain_head_at_export": "708a4c1f08295a4a004bff41d0cd61c7fe69743f25411893965a5e50afa34583",
  "recipient": "internal-audit-evaluation"
}
```

PAYLOAD_SHA256
26d186b23ca72cce8da1e7480f984f06ad192ed662b42266d113961e0835f23e

PREV_HASH
708a4c1f08295a4a004bff41d0cd61c7fe69743f25411893965a5e50afa34583

ENTRY_HASH
0677292fd37ebd2d023d0ffd56cc42915054b69b0dbd5ba8e80764553b9cabcb

ENTRY ULID	O1M2PX7S1O1EO2SZQGNAPWQH2R
ACTOR	T. Bergstrom (0000000000VMH36H2NCSVRH680)
ROLE AT TIME OF ACTION	SECURITY_OFFICER
SUBJECT	ledger_partition audit_ledger_2026_09 · version —
REQUEST ID	req-fb4e28989830
SOURCE IP	10.14.8.50
RATIONALE	Chain head flushed to Object Lock in compliance mode. Retention cannot be shortened, including by the account root.

CANONICAL PAYLOAD (THE BYTES THAT WERE HASHED)

```
{
  "flush_trigger": "batch_size",
  "partition_name": "audit_ledger_2026_09",
  "entries_flushed": 11,
  "worm_object_key": "s3://magellan-audit-sample/partitions/audit_ledger_2026_09.ndjson",
  "worm_object_lock": "compliance mode, 7-year retention",
  "sse_kms": "arn:aws:kms:us-east-1:000000000000:key/sample-0000-0000"
}
```

PAYLOAD_SHA256
f5f2619b8100f8c7a713cd75d724f1f7794b226abaeaf952f3529fac04180643

PREV_HASH
0677292fd37ebd2d023d0ffd56cc42915054b69b0dbd5ba8e80764553b9cabcb

ENTRY_HASH
fb549d38c456c1a09f73f5f2d306fdec3e01419a7ef80171443f8a42daf02ac4

Partition seal & WORM head

A detached partition has to stay verifiable on its own, so the first and last hash of every partition are recorded separately from the entries themselves.

Partition head

PARTITION	audit_ledger_2026_09
FIRST ULID	O1M2P7HT00XZWG4H29YN3PZ7AZ
LAST ULID	O1M2PX7S101EO2SZQGNAPWQH2R
FIRST HASH	3dca562ce21a3b1f3ee9c06ad362dc39c7443ee89f6f4455a100f409e5f6e97a
LAST HASH	fb549d38c456c1a09f73f5f2d306fdec3e01419a7ef80171443f8a42daf02ac4
ENTRY COUNT	11
SEALED AT	2026-09-17T05:25:40.000Z
OBJECT KEY	s3://magellan-audit-sample/partitions/audit_ledger_2026_09.ndjson

WORM chain head

FLUSH ULID	O1M2PX7S101EO2SZQGNAPWQH2R
AS OF	2026-09-17T05:25:40.000Z
TAIL ULID	O1M2PX7S101EO2SZQGNAPWQH2R
HEAD HASH	fb549d38c456c1a09f73f5f2d306fdec3e01419a7ef80171443f8a42daf02ac4
KMS KEY	arn:aws:kms:us-east-1:000000000000:key/sample-0000-0000

Why the seal matters commercially. A ledger your own team can quietly rewrite is not evidence — it is a database with extra steps. Object Lock in compliance mode with a fixed retention period removes the ability to shorten retention from everyone, including the account root. That is the difference between a claim you have to take on trust and a property you can inspect.

Verifying it yourself

The pack ships with a verifier that uses nothing but the Python standard library — no API keys, no network, no database, no Magellan software running. It re-derives every hash from the payloads printed in Section 03.

```
$ python3 verify_chain.py magellan_sample_evidence_pack.json
```

EXPECTED RESULT

```
[PASS] #01 SchemaIngested ... [PASS] #11 WormHeadFlushed
[PASS] partition last_hash = final entry
[PASS] WORM head = recomputed chain head
[PASS] ULIDs strictly increasing
```

RESULT: CHAIN INTACT — every hash re-derived from the payloads shown.

Try to break it. Run the verifier with `--tamper` and it changes one number inside one entry's payload — a single character — then reports the chain broken from that entry onward. Change one character of a rationale, an approval timestamp, or a rejected link, and every hash after it stops matching. There is no way to edit the past in this structure without leaving a mark on it.

What this proves, and what it does not

PROVES

- The record was not altered after it was written.
- Entries cannot be inserted, removed, or reordered silently.
- The approval order is fixed, not merely asserted.
- The evidence can be checked without vendor cooperation.

DOES NOT PROVE

- That the events themselves were true when recorded.
- That the actor identities were correct at write time.
- That the mapping produced a correct output file.
- Anything about this sample's synthetic scenario.