

## SPHEREON APPLICATION NOTE

# Evidence and Auditability for Digital Transformation Processes

---

*How events, evidence, and protected records preserve why a decision was justified, long after it was made*

Evidence and auditability are the discipline of deciding in advance what must be provable about a decision, capturing it as the decision happens, protecting it, and retaining it for as long as the obligation lasts.

Version 0.3 | July 2026



## Contents

### Section

1. Executive summary
2. Purpose, audience, and example
3. Practical benefits of evidence and auditability
4. What evidence and auditability are
5. How evidence and auditability work
6. An example: care authorization on behalf of a patient
7. Evidence objects and reconstruction matrix
8. How this maps to the Sphereon stack
9. Recommended first engagement
10. Summary

Appendix: glossary

## 1. Executive summary

Evidence and auditability should be understood as a design decision taken before a process runs, not as a reporting exercise carried out afterwards.

Most organizations already log a great deal. Systems record what they did, when, and messages, like whether something succeeded. That is necessary but it is not the same as being able to defend a decision. Logs describe system behaviour. A supervisor, auditor, or court asks a different question: on what basis was this decision justified at the moment it was taken.

The gap appears months later. The records show that a decision was made. They do not show which rule or policy was in force at the time, which evidence was accepted, whose authority was relied on, or why that combination was considered sufficient. Nothing was deleted and nothing failed. The information was simply never captured, because nobody knew in advance which question would be asked.

Evidence and auditability close that gap. The organization decides in advance which questions it must be able to answer, captures the events and decision records that answer them, links evidence to trust decisions and policy versions, protects those records against alteration, and retains them for as long as the obligation lasts. The result is not more data. It is a smaller set of records that actually answers the question.

This applies wherever a decision must survive scrutiny: healthcare authorization and reimbursement, financial services, public services, licensing, procurement, and other exchanges of data. This note uses a care authorization requested on behalf of a patient as the running example, because it combines mandate, eligibility, professional accreditation, and special-category data in a decision that is reviewed as a matter of routine.

*For Sphereon, evidence and auditability are where a decision becomes durable: the platform records what happened, why it was permitted, and under which policy, and keeps that account verifiable long afterwards.*

### What the board gains

- **Decisions that survive review.** Evidence, trust decision, policy version, mandate, and outcome are linked to one case, so a decision can be explained without relying on staff memory or manual reconstruction.
- **Lower cost of audit and investigation.** Answering a supervisor becomes a query rather than a project, because the record was designed around the question.
- **Demonstrable integrity.** Records are append-only and tamper-evident, so the organization can show that the account of a decision has not been altered after the fact.
- **Proportionate data handling.** Capturing what is necessary, redacting what is sensitive, and retaining for a defined period is a stronger privacy position than logging everything indefinitely.

## The ask

We ask you to consider sponsoring one focused evidence-and-auditability accelerator on a single high-value decision, not an organization-wide logging or archiving programme.

The proposed accelerator is a four-week, fixed-scope engagement that establishes which questions the organization must be able to answer about that decision, and whether it can answer them today.

Section 9 sets out the scope, timeline, and decision.

Success is measured in operational terms: the proportion of material decisions for which a complete account exists, the time required to reconstruct a decision on request, the completeness of evidence and policy-version linkage, and the ability to demonstrate that records have not been altered. Ownership sits jointly with business, risk, compliance, privacy, and architecture, because deciding what must be provable is a business and legal judgment, not only a technical one.

Our consultancy partner will lead discovery and the design of the evidence requirements; Sphereon provides the trust infrastructure, connector architecture, event and audit layer, and reconstruction capability.

## 2. Purpose, audience, and the example

This application note explains what evidence and auditability mean in practice, why organizations need them, and how they can be operationalized in digital trust processes.

The intended readers are application managers, line managers, process owners, compliance leads, risk teams, privacy officers, architects, and delivery partners.

It is not primarily a document about healthcare or any other specific sector, but healthcare is provided a good example. A care authorization requested on behalf of a patient is used as the running example because it is reviewed routinely rather than only after an incident, and because it combines mandate, eligibility, accreditation, and sensitive data in one recognizable decision.

### What this note covers

- What evidence and auditability mean in a business process context.
- How they differ from application logging, monitoring, and reporting.
- How events, decision records, linkage, integrity, and retention fit together.
- How the method can be illustrated through a care authorization decision.
- How evidence and auditability can be operationalized in the Sphereon stack.

### What this note does not cover

- It does not define a complete records-management or archiving architecture.
- It does not prescribe a specific retention period, which depends on the applicable obligation.
- It does not replace legal advice on what an organization is required to retain.
- It does not claim that good records remove the need for sound decisions. It makes the decisions that were taken explainable.

### 3. Practical benefits of evidence and auditability

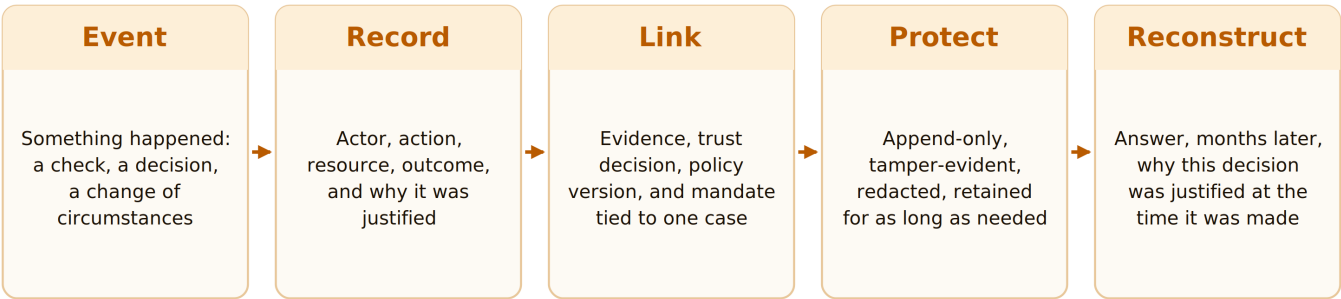
Evidence and auditability are the discipline of deciding in advance what must be provable about a decision, capturing it as the decision happens, protecting it, and retaining it for as long as the obligation lasts. They are easier to understand when the practical benefits are clear before the mechanism is introduced in detail.

Table 1. Practical benefits for business and application teams

| Benefit                                  | Practical meaning                                                                                                                       |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Faster answers to auditors               | A request for the basis of a decision is answered from a linked record, instead of assembling evidence from several systems and people. |
| Less dependence on memory                | The reason a decision was justified survives staff changes, system migrations, and reorganizations.                                     |
| Clear separation of signal and proof     | Real-time events drive operations; durable records support later investigation. Each is designed for its own purpose.                   |
| Demonstrable integrity                   | Records can be shown to be unaltered, which is a stronger position than asserting that nobody would have changed them.                  |
| Proportionate retention                  | Records are kept for a defined period tied to the obligation, rather than indefinitely by default or deleted by accident.               |
| Sensitive data handled deliberately      | Secrets and credentials are removed before storage, so the audit trail does not become a new source of exposure.                        |
| Faster reaction to changed circumstances | A withdrawn mandate or revoked credential is itself an event, so later decisions can take it into account.                              |
| Reusable across processes                | The same event, record, and reconstruction pattern serves many decisions instead of being rebuilt per application.                      |

The central point is simple: **evidence and auditability close the gap between a decision that was made and a decision that can be defended.** They help an organization avoid the situation where everything was recorded and nothing can be explained.

Figure 1. The evidence and auditability chain



## 4. What evidence and auditability are

In simple terms, evidence and auditability mean deciding in advance what an organization must be able to prove about a decision and capturing it as the decision happens. That is the simple version.

### A short failure example to clarify the problem

A care provider requests authorization to deliver treatment on behalf of a patient. The request is checked, approved, and the care is delivered and reimbursed. Eighteen months later a payer review selects the file. The reviewer asks a single question: on what basis was this provider allowed to act for this patient, and was the treatment eligible under the rules in force at that time? Nobody can answer.

No system failed. System actions were logged. The portal recorded that a request was submitted. The workflow recorded that it was approved and by whom. The reimbursement system recorded the payment. The logs are complete and nothing was deleted.

What is missing is the reason: which mandate was valid that day, which version of the eligibility rules applied, which accreditation was accepted as sufficient, and who or what determined that the combination was enough.

This is why the familiar instinct does not help here. The instinct says: log more, or keep logs longer. But the organization already had complete logs and kept them. More of the same records would have produced more evidence that a decision occurred, and still no evidence that it was justified. The missing layer was never volume. It was that nobody decided in advance which question would be asked, so nothing was captured to answer it. That is the gap evidence and auditability are built to close, and the rest of this section explains how.

Evidence and auditability go beyond recording that something happened. They capture the account of why an outcome was permitted: the evidence relied upon, the source that was trusted, the rule that applied and the version it was in, the authority that was exercised, and the outcome that followed. That account is then protected against alteration and retained for as long as the obligation lasts.

#### Plain-language definition

Evidence and auditability are the deliberate capture, linkage, protection, and retention of the account of a decision: what happened, on what evidence, under which policy, by whose authority, and with what outcome, so that it can be reconstructed and defended long afterwards.

Application logging answers a narrow question: what did this system do, and did it work. That is necessary for operations and troubleshooting. It is not the same question as whether a business decision was justified. A complete technical log can describe every step of a process that reached the wrong conclusion for reasons the log never captured.

A simple distinction: a log says an approval was recorded at a particular time. An audit record says this decision was permitted on this evidence, from this trusted source, under this version of this rule, by this authority, and here is how that can be checked.

### **Why events and audit records are not the same thing**

Events and audit records serve different purposes and should be designed separately. Events are real-time signals: they tell other parts of the organization that something has happened, so workflows can start, caches can update, and risk signals can propagate. They are optimized for immediacy.

Audit records are durable accounts, written to be read months or years later by someone who was not present. They are optimized for reconstruction. Treating one as a substitute for the other is a common and expensive mistake: a stream of events is difficult to defend a decision with, and an audit archive is too slow to run operations from.

### **Typical ambiguity without designed evidence**

- Logged may mean a technical event was recorded, or that the reason for an outcome was preserved.
- Approved may mean a system recorded an outcome, or that a named authority accepted responsibility under a specific rule.
- Evidence may mean a document was received, or that a claim from a trusted source was verified and relied upon.
- Traceable may mean the sequence of steps can be followed, or that the justification for each step can be explained.
- Retained may mean data still exists somewhere, or that a complete and unaltered account is available for the required period.

Without designed evidence, organizations may hold large volumes of records while still being unable to answer the one question that matters when a decision is challenged.



## 5. How evidence and auditability work

A useful evidence model usually defines six practical elements: the question, the event, the decision record, the linkage, the integrity guarantee, and the retention rule. These elements can be used in any high-trust process.

Table 2. Core elements of an evidence and auditability model

| Element            | What it defines                                                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| The question       | What the organization must be able to answer later, and to whom. This is decided before the process runs, not after.                                     |
| Event              | A business-significant occurrence: a check performed, a decision taken, an authority granted or withdrawn, a circumstance changed.                       |
| Decision record    | The durable account of an outcome: actor, action, resource, result, and the reason it was permitted or refused.                                          |
| Linkage            | The connections that make the record meaningful: evidence to trust decision, decision to policy version, action to mandate, and all of them to one case. |
| Integrity          | The guarantee that the record has not been altered since it was written, and the means to demonstrate that.                                              |
| Retention & access | How long the account must survive, who may read it, and what must be removed or redacted before it is stored.                                            |

### The model turns business questions into operational checks:

- Which questions must we be able to answer about this decision, and for how long?
- Which events are business-significant, as opposed to merely technical?
- What must each decision record contain to be defensible on its own?
- Which evidence was relied upon, and which source was trusted for it?
- Which version of which rule was in force at the moment of the decision?
- Whose authority or mandate was exercised, and was it valid at that time?
- How is the record protected against later alteration?
- What sensitive data must be removed before the record is stored?
- How long must this be retained, and what happens at the end of that period?
- How quickly can a complete account be produced on request?

This is the operational value: the model is not only a records policy. It becomes the layer that governs which events are emitted, what each decision record contains, how records are linked and protected, and how an account is reconstructed on demand.

## 6. An example: care authorization on behalf of a patient

The following example illustrates the method. The same approach can be applied to many other decisions, such as credit approval, supplier award, licence issuance, benefit eligibility, or any action taken by a software agent on behalf of an organization.

### The business case

A care provider requests authorization from a payer to deliver treatment on behalf of a patient. The decision depends on the provider's mandate to act for that patient, the patient's eligibility, the provider's accreditation for this treatment, and the rules in force at that moment. The decision is reviewed routinely, and it involves special-category personal data, so the account of it must be both complete and proportionate.

#### 6.1 Deciding the questions in advance

Before the process is built, the organization decides which questions it must be able to answer about this decision, to whom, and for how long. This is the step most often skipped, and the reason later reconstruction fails.

- Who will ask about this decision: payer, supervisor, patient, or court?
- What will they ask, and what would a complete answer contain?
- How long does the obligation to answer last?

**Evidence output:** The organization has an explicit list of questions the record must answer, which determines everything captured downstream.

#### 6.2 Events during the decision

As the request is handled, business-significant occurrences are emitted as events: the mandate was presented and checked, eligibility was confirmed, accreditation was verified, the policy was evaluated, and the outcome was reached.

- Which occurrences are business-significant rather than merely technical?
- Does each event carry the case, the actor, and the moment it occurred?
- Are events emitted for refusals and exceptions, not only for approvals?

**Evidence output:** The process produces a stream of meaningful events that can drive workflow immediately and feed the durable record.

### 6.3 The decision record

At the point of decision, a durable record is written. It states the outcome and the reason for it, distinguishing between a refusal on policy grounds, a failure to establish authority, and a technical error, because these are different findings for a reviewer.

- What was decided, by whom or by what, and on which case?
- Was the outcome an approval, a refusal on policy grounds, or a failure to establish authority?
- Which rule produced that outcome, and in which version?

**Evidence output:** The outcome is recorded together with its justification, not only as a status change.

### 6.4 Linking evidence, trust, and authority

The record is linked to the evidence relied upon, the source trusted for that evidence, the mandate exercised, and the policy version in force. Without these links the record states a conclusion but cannot support it.

- Which evidence supported each element of the decision?
- Which issuer or source was accepted as trustworthy for that evidence, and why?
- Which mandate authorized the provider to act for this patient, and was it valid at that moment?

**Evidence output:** A reviewer can follow the decision back to the evidence and authority that justified it, rather than inferring them.

### 6.5 Protecting and retaining the account

Sensitive values are removed before storage. The record is written to append-only storage, protected so that later alteration can be detected, and retained for the period the obligation requires.

- What must be redacted so the audit trail does not become a new exposure?
- How would an alteration to this record be detected?
- How long must this account survive, and what happens at the end of that period?

**Evidence output:** The account is durable, proportionate, and demonstrably unaltered for as long as it is needed.

## 6.6 Retrieval on request

Because the account was captured and linked as the decision happened, it already exists as a complete record before anyone asks for it. When a reviewer requests the basis of this authorization months later, nothing has to be rebuilt: the organization retrieves the account for that case as a unit, the events, the decision and its reason, the evidence and trust decisions, the mandate, and the policy version in force.

- Can the complete account for one case be retrieved as it was recorded, rather than rebuilt from separate systems?
- Does the account answer the questions identified at the start?
- Can the organization demonstrate that the record has not been altered since it was written?

**Evidence output:** the organization answers a review from a record that was complete at the time of the decision, not assembled afterwards, and can show the answer is trustworthy,

### Operational test

A useful test for any decision is this: if a reviewer asks in eighteen months why this outcome was justified, can the organization produce a complete and unaltered account from its records, without depending on the people who were involved at the time?

## 7. Evidence objects and reconstruction matrix

The following objects are examples from the care authorization case. They should be read as practical model building blocks, not as database-table names. The same pattern can be reused in other domains with different object names.

**Table 3. Example evidence objects**

| Object                  | Business meaning                                                            | Why it matters                                                       |
|-------------------------|-----------------------------------------------------------------------------|----------------------------------------------------------------------|
| <b>AuditQuestion</b>    | A question the organization must be able to answer later, and for how long. | Determines what must be captured, before anything is built.          |
| <b>BusinessEvent</b>    | A business-significant occurrence during the process.                       | Separates meaningful occurrences from technical noise.               |
| <b>DecisionRecord</b>   | The durable account of an outcome and the reason for it.                    | Carries the justification, not only the status.                      |
| <b>EvidenceLink</b>     | The connection between a decision and the evidence relied upon.             | Allows a conclusion to be traced to its support.                     |
| <b>TrustDecision</b>    | The determination that a source was acceptable for this evidence.           | Shows why the evidence was believed, not just that it existed.       |
| <b>PolicyVersion</b>    | The specific version of the rule in force at the moment of decision.        | Prevents a decision from being judged against rules written later.   |
| <b>MandateReference</b> | The authority under which an actor acted for another party.                 | Answers the question of who was allowed to act, and on whose behalf. |
| <b>CaseCorrelation</b>  | The identifier that ties all records for one case together.                 | Makes reconstruction a retrieval rather than an investigation.       |
| <b>IntegrityProof</b>   | The means by which alteration of a record can be detected.                  | Turns an assertion of trustworthiness into something demonstrable.   |
| <b>RetentionRule</b>    | How long the account is kept, and what is redacted or removed.              | Keeps retention proportionate and defensible under privacy law.      |

The next table shows how the questions a reviewer asks to connect to what must be captured and how it is reconstructed. This is where evidence and auditability become operational.

**Table 4. Question, evidence, and reconstruction matrix**

| <b>Question asked later</b>                   | <b>What must be captured</b>             | <b>Where it comes from</b>                    | <b>How it is reconstructed</b>                                      |
|-----------------------------------------------|------------------------------------------|-----------------------------------------------|---------------------------------------------------------------------|
| Who acted, and on whose behalf?               | Actor identity and the mandate exercised | Identity layer, mandate registry              | Retrieve the decision record and its mandate reference for the case |
| What evidence supported this?                 | Evidence items and their sources         | Credentials, registries, partner systems      | Follow the evidence links from the decision record                  |
| Why was that evidence believed?               | The trust decision for each source       | Trust configuration in force at that time     | Retrieve the trust decision recorded alongside the evidence         |
| Which rule applied?                           | Policy identifier and version            | Policy layer at moment of evaluation          | Read the policy version captured on the decision record             |
| Was the outcome approval or refusal, and why? | Result type and reason                   | Decision layer                                | Read the outcome and its distinguishing reason code                 |
| Has the record been altered since?            | Integrity proof over the record          | Integrity mechanism applied at write time     | Verify the record against its integrity proof                       |
| Is the account complete for this case?        | Case correlation across all records      | Correlation applied to every event and record | Retrieve all records sharing the case correlation identifier        |

## 8. How this maps to the Sphereon stack

In a Sphereon-based implementation, evidence and auditability become the durable memory of the process. The platform records what happened and why it was permitted, protects those records, and makes them retrievable long afterwards.

Table 5. Operationalizing evidence and auditability in the Sphereon stack

| Sphereon layer       | Role in the process                                                                                                                                                                                       |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Event layer          | Emits business-significant events for identity, authorization, and lifecycle changes, carrying case, actor, tenant, and correlation context so that operations and records draw on the same occurrences.  |
| Audit layer          | Writes durable, append-only records of every command and decision, including the actor, the resource, the outcome, and whether a refusal was a policy denial, an authority failure, or a technical error. |
| Correlation layer    | Applies a correlation identifier across the records belonging to one case, so a complete account can be retrieved as a unit instead of assembled by hand.                                                 |
| Integrity layer      | Protects records with hash chaining and periodically signed checkpoints, so that alteration is detectable, and integrity can be demonstrated for a range of records.                                      |
| Redaction layer      | Removes sensitive values such as credentials and tokens before records are stored, so the audit trail does not become a new source of exposure.                                                           |
| Retention layer      | Retains records for a configured period tied to the obligation and removes them when that period ends.                                                                                                    |
| Signal layer         | Receives and propagates changes of circumstance, such as a withdrawn authority or a compromised credential, so that later decisions and existing sessions can take them into account.                     |
| Reconstruction layer | Answers structured queries by case, actor, outcome, or period, so that a review request is served from records rather than from memory.                                                                   |

This means evidence and auditability are not a reporting feature bolted on at the end. They are part of the operating architecture: they determine which events are emitted, what each record contains, how records are linked and protected, and how an account is produced when someone asks.

The design principle throughout is that recording must not endanger the operation it records. Audit capture is built to degrade gracefully rather than to block the business process it observes.

## 9. Recommended first engagement

### The ask

Approve a four-week, fixed-scope accelerator on one high-value decision. It is designed to establish, at limited and bounded cost, which questions the organization must be able to answer about that decision and whether it can answer them today, before any larger commitment is made. It is a decision to learn, not a decision to build an archive.

The accelerator deliberately does not try to govern every record in the organization. It selects one decision that is reviewed in practice, and produces the question set, the evidence model, and the reconstruction design for that decision. At the end, the organization has enough evidence to decide whether to stop, extend to the next decision, or move to implementation.

### Suggested scope

- One decision that is subject to real review, such as an authorization, an award, or an eligibility determination.
- One business unit or process owner.
- One set of questions that must be answerable, with their retention obligations.
- One evidence, trust, and mandate model for that decision.
- One reconstruction requirement, expressed as a request the organization must be able to serve.

Table 6. Example 4-week evidence and auditability accelerator

| Phase    | Focus                           | Output                                                                                |
|----------|---------------------------------|---------------------------------------------------------------------------------------|
| Week 1   | Questions and obligations       | The list of questions that must be answerable, their audiences, and retention periods |
| Week 2   | Events and decision records     | Event model, decision record content, and reason codes for outcomes                   |
| Week 3   | Linkage, integrity, and privacy | Evidence, trust, policy version and mandate linkage; integrity and redaction design   |
| Week 4   | Sphereon implementation mapping | Reconstruction design, retention mapping, and gap assessment against current systems  |
| Optional | Prototype definition or build   | Prototype backlog or working reconstruction of one decision in the Sphereon stack     |

### Division of labor with a consultancy partner

Our consultancy partner can lead business discovery, the design of the question set, stakeholder alignment, and the mapping of legal and regulatory obligations to retention requirements. Sphereon can provide the reference architecture, event and audit components, integrity and redaction mechanisms, correlation model, and reconstruction capability.

### Practical positioning

The partner determines what must be provable. Sphereon makes it provable, and keeps it that way.



## 10. Summary

Evidence and auditability are the discipline of deciding in advance what must be provable about a decision, capturing it as the decision happens, protecting it, and retaining it for as long as the obligation lasts.

They answer the question that logging alone leaves open: not what the systems did, but why the outcome was justified at the time.

The care authorization example shows the method in practice. An organization does not only need a record that an authorization was granted. It needs the mandate, the eligibility evidence, the trusted sources, the policy version, and the outcome linked as one account, protected against alteration and retrievable months later.

For Sphereon and its partners, evidence and auditability create a reusable consultancy and implementation pattern: start with one decision that is genuinely reviewed, establish the questions it must answer, model the events and records that answer them, and then operationalize that model through the event, audit, integrity, retention, and reconstruction layers of the platform.

## Appendix: glossary

| Term                   | Business-language meaning                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Evidence by design     | Deciding in advance what evidence is necessary and proportionate to justify a decision later.                         |
| Audit record           | A durable account of an outcome, the reason and context why it was permitted or refused.                              |
| Event                  | A (business-significant) occurrence, triggering a signal, so other processes or parts of the organization may react.  |
| Correlation identifier | A value shared by all records belonging to one case, enabling complete retrieval.                                     |
| Policy version         | The specific version of a policy rule that was in force at the moment a decision was taken.                           |
| Mandate                | The authority for a person, organization, system, or agent, to act on behalf of another party within a defined scope. |
| Append-only            | Storage system in which records can only be added and read but not changed or removed.                                |
| Tamper evident         | A mechanism that makes alteration of a stored record detectable.                                                      |
| Hash chaining          | Linking each record to the previous one so that any modification breaks the chain, making it tamper evident.          |
| Redaction              | Removing sensitive values from a record before it is (permanently) stored.                                            |
| Retention period       | The length of time a record must be kept in order to meet an obligation.                                              |
| Reconstruction         | Producing a complete account of a past decision from stored records.                                                  |