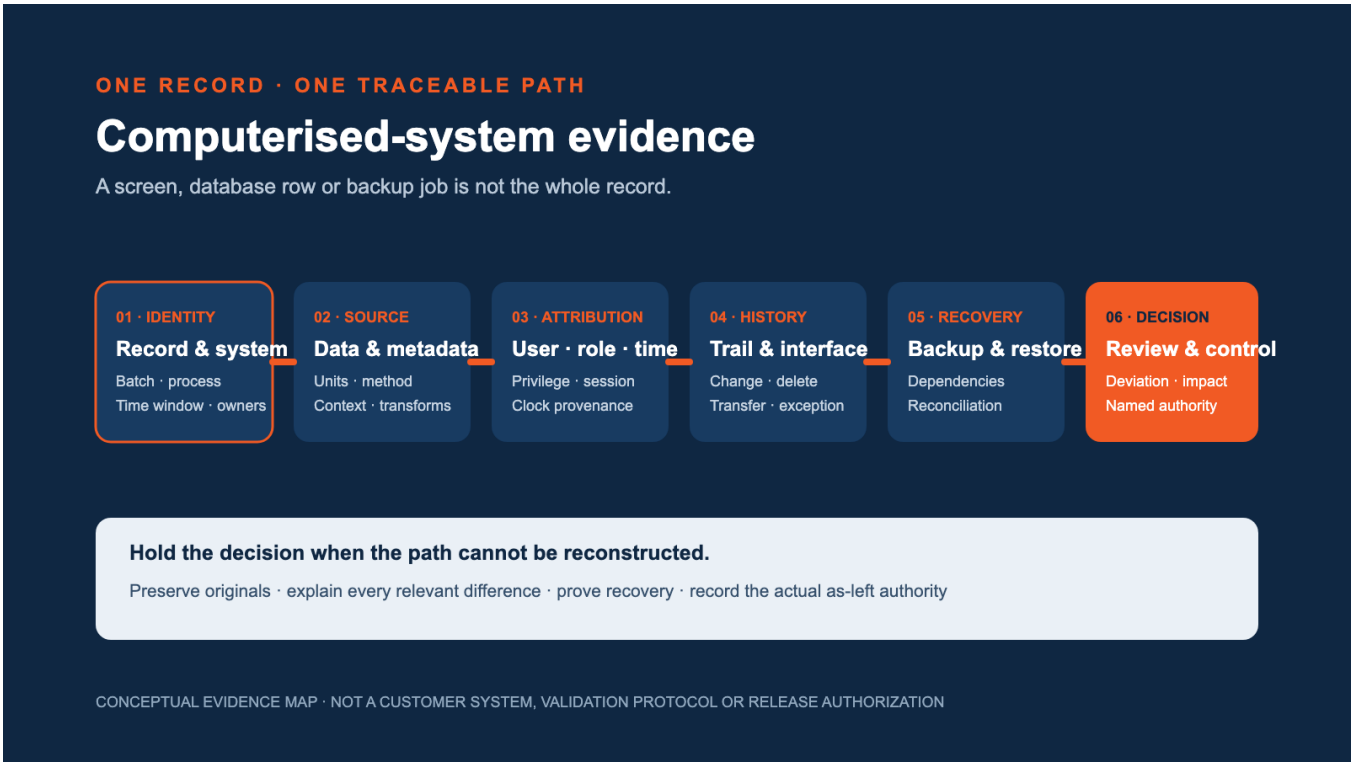
EN-GUIDE-08 | PHARMACEUTICAL COMPUTERISED SYSTEMS

Data Integrity, Audit Trail, Backup, Restore & Review Evidence

A value on an HMI, a database row or a completed backup job does not by itself prove a complete, consistent and accurate GMP record. Fix the record and system boundary, preserve source evidence and metadata, reconcile time and interfaces, review relevant audit trails, prove recovery and place the final decision with named system, record and quality owners.

Reviewed	23 July 2026	**Audience**	Quality, CSV, IT/OT, automation and production teams
Systems	PLC, SCADA, historian, MES, laboratory and interfaces	**Output**	Reviewable record and recovery evidence package



Decision summary

A stored value or green backup status is not integrity or recovery proof.
Trace one relevant record from identity and source data through user, time, audit trail, interfaces, restore and accountable quality review.

OBSERVABLE TRIGGERS

Require record-path evidence when any of these conditions appear

- HMI, PLC, SCADA, historian, laboratory system, MES or interface values, timestamps, users or batch context conflict.
- Data can be changed, deleted, repeated or exported without a visible reason, reviewer or affected-record link.
- Shared accounts, unmanaged administrator access, inactive users or role differences obscure attribution.
- Clock offset, time-zone handling, sequence resolution or interface delay prevents reliable event ordering.
- A backup job is green, but scope, dependencies, metadata, interfaces or post-restore reconciliation are unproven.
- Review covers a report while source data, metadata, audit trail, interface failures or aborted runs remain outside scope.

STOP-WORK CONDITIONS

Preserve the controlled state when evidence may be lost or misattributed

Boundary unknown	System, instrument, record, product, batch, process step, equipment, time window or owner cannot be fixed.
Original at risk	Reset, overwrite, migration, restore, service action or log rotation could obscure source data or metadata.
Authority unclear	Shared credentials, unknown sessions, unmanaged privileges or absent approval prevent attribution.
Time unresolved	Clock source, offset, zone, sequence resolution or interface delay is unknown.
Recovery unproven	Backup content, versions, dependencies, licenses, keys, configuration or reconciliation are incomplete.
Review owner absent	Exceptions, deviations, affected batches, restrictions or acceptance authority remain outside review.

Stop means preserve and escalate

Protect available source records and configuration, maintain the authorized hold, document unavoidable preservation actions and return the decision to the named site authority.

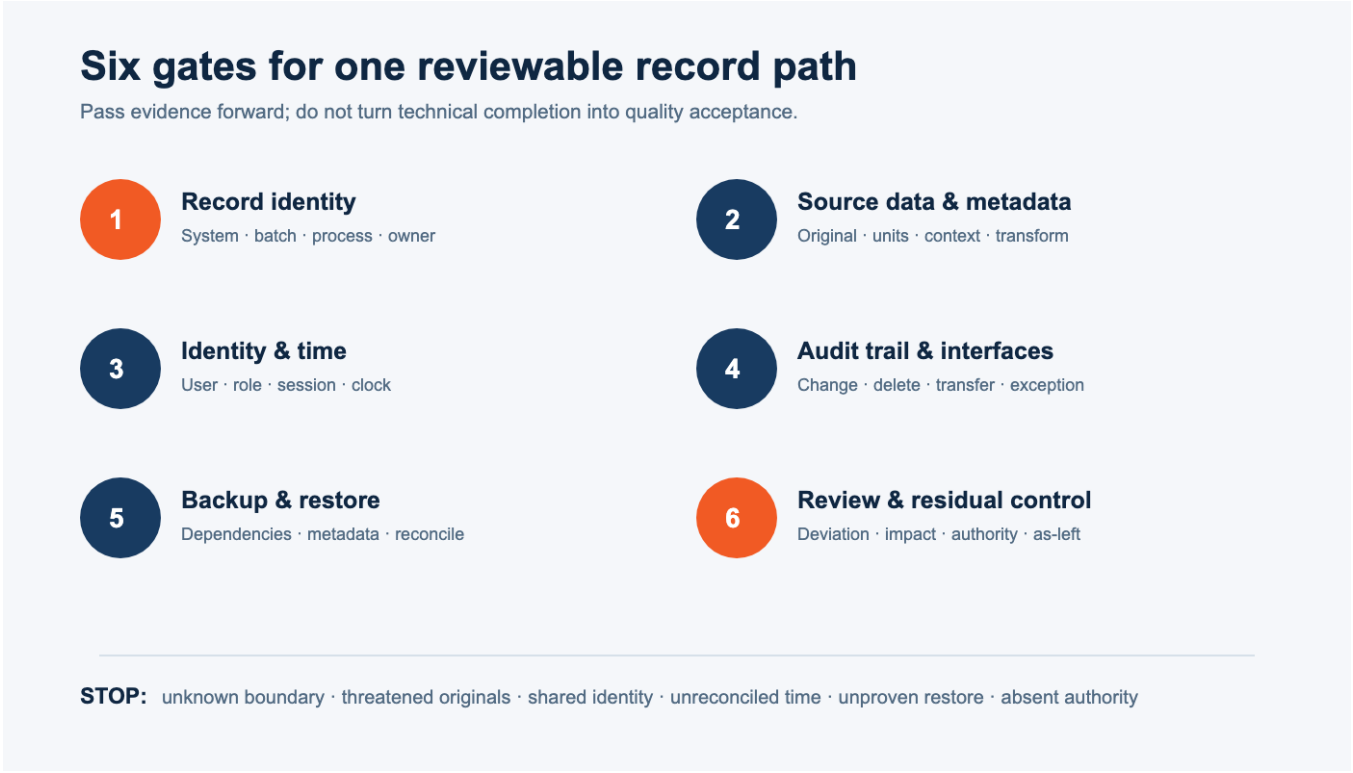
PRE-WORK COLLECTION

Fix the record-generating boundary before judging trustworthiness

Collect	Minimum evidence	Why it matters
Record identity	Site, system/instrument, record type and ID, product/batch/process, equipment, event window, status and owners	Prevents different records or batches being merged.
Source and metadata	Original entry, raw signal/file, units, method, user, timestamps, sequence, context, calculations and transformations	Supports reconstruction from generation to result.
Access and audit trail	Accounts, roles, privileges, sessions, administrator actions, create/modify/delete events, reasons and review	Connects actions to authorized identities.
Interfaces and time	Source/destination tags, queues, acknowledgements, retries, failures, clocks, offsets, zones and sequence resolution	Shows whether transfer or time changed meaning.
Backup and restore	Scope, schedule, success evidence, configuration, versions, dependencies, retention, restore method and test result	Separates file existence from recoverability.
Review and decision	Review scope, exceptions, deviations, affected records/batches, reviewer, restrictions, approval and residual ownership	Makes the final accountable decision visible.

SIX EVIDENCE GATES

Follow one relevant record from generation to accountable review



Gate	Evidence to close	Hold when
1. Record identity	Record, system, product/batch/process, equipment, time window and owners describe the same activity.	Boundary or owner is missing.
2. Source and metadata	Original or verified true-copy evidence retains context, units, method, user, time and transformations.	Only a screenshot or unexplained export remains.
3. Identity and time	Unique user/role, authorization, session and clock provenance support attribution and sequence.	Shared access or time gaps remain.
4. Audit trail and interfaces	Relevant changes, deletions, repeats, failures and transfers are reviewed with reasons and affected records.	Exceptions sit outside review scope.
5. Backup and restore	Approved content restores with dependencies, metadata and interface/data reconciliation.	Backup success is the only recovery proof.
6. Review and control	Deviations, affected batches, restrictions, validation status, decision and residual owners are recorded.	Technical completion is treated as quality acceptance.

EIGHT-STEP EVIDENCE PROCEDURE

Test the record path without changing the evidence first

01	**Fix record and system identity.** Name the record, source device/application, product/batch/process, equipment, time window, current status and owners.
02	**Preserve source data and metadata.** Secure the original or controlled true copy, context, units, method, configuration, raw files, logs and export method.
03	**Reconcile user, role and privilege.** Map each relevant action to a unique identity, authorized role, session and approval; preserve privileged activity.
04	**Establish time provenance.** Record clock source, synchronization, offset, zone, daylight-saving handling, event resolution and known delay.
05	**Review audit trails and exceptions.** Include create/modify/delete, reasons, repeated or aborted runs and unexplained gaps in an approved risk-based scope.
06	**Trace interfaces end to end.** Compare source and destination identity, value, units, quality, timestamp, acknowledgement, retry and reconciliation.
07	**Prove backup and restore.** Restore an approved scope in an authorized boundary and verify configuration, metadata, permissions, dependencies and completeness.
08	**Review, disposition and hand over.** Connect findings to deviations, affected records/batches, restrictions, quality decision, as-left state and ownership.

EXPERT REVIEW

Questions before a convenient record becomes supported evidence

- Can a reviewer reconstruct who did what, when, why and under which approved method from retained source and metadata?
- Does the result remain linked to the generating instrument, configuration, calculation, transformation and affected batch?
- Are privileged access, repeated runs, aborted sequences and deletions visible to the approved review scope?
- Can events across PLC, SCADA, historian, MES and laboratory systems be ordered without guessing?
- Does recovery prove application/configuration compatibility, users/roles, metadata, interfaces and reconciliation?
- Are technical repair, validated state, record acceptance and batch disposition kept as separate named decisions?

AS-LEFT HANDOVER

Transfer the evidence, limitations and authority that remain

Identity and provenance	Recovery and decision
- System, record and batch identity - Source data and metadata - User, role, time and audit trail - Interfaces, calculations and transformations	- Backup scope and actual restore test - Reconciliation and exceptions - Deviations, restrictions and monitoring - Quality decision, open items and owners

Decision record

Name the affected record and batch scope, validation status, residual restriction, monitoring condition, rollback state and accountable system, record and quality owners.

OFFICIAL PRIMARY SOURCES

Use each source within its published jurisdiction and approved site framework

1. **eCFR 21 CFR Part 11**
   https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11
   United States regulatory text for electronic records and electronic signatures; confirm predicate-rule applicability.
2. **FDA Data Integrity and Drug CGMP**
   https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-integrity-and-compliance-drug-cgmp-questions-and-answers
   United States final guidance for drugs, including biologics.
3. **European Commission EU GMP Annex 11**
   https://health.ec.europa.eu/document/download/8d305550-dd22-4dad-8463-2ddb4a1345f1_en
   European Union GMP guidance for computerised systems; confirm the current Volume 4 publication.
4. **NIST SP 800-82 Rev. 3**
   https://csrc.nist.gov/pubs/sp/800/82/r3/final
   Operational technology security guidance, not a pharmaceutical validation or batch-release standard.

Application limit

Confirm country, predicate rules, product authorization, pharmacopoeia, AHJ, site quality system, approved SOPs, validation/qualification plan, retention schedule, cybersecurity policy, OEM support and qualified reviewers. This guide supplies no universal audit-trail review frequency, retention duration, validation acceptance value or batch-release authority.

Field Electric Guide | Reviewed 23 July 2026 |
https://elechubs.com/en/guides/pharmaceutical-computerised-systems-data-integrity-audit-trail-backup-restore-review-evidence