Reliable Context

RELIABLE CONTEXT / RESEARCH & PRACTICAL GUIDANCE

Audit Trail Review in GxP: Capture, Protect, Review

> Reliable Context is a kernel of truth: a system of record for organizations that fuse private and public information and must defend every value they act on. One canonical record per real thing, a cited source and an observation date behind every value, unknowns declared rather than left blank, and any past state of the record reproducible.

Published by Reliable Context · 2026-10-29 · audit trail review · gxp audit trail requirements · audit trail annex 11 · audit trail review procedure · electronic audit trail fda

Original article: https://reliablecontext.com/articles/audit-trail-review-part-11-annex-11-what-to-capture-and-review



In this article

1. Generate, protect, review: three duties that get conflated
2. Duty 1: what a useful audit trail contains
3. Reason for change and old/new values
4. Duty 2: protecting the trail from the people it records
5. Duty 3: review — scope, frequency, and who
6. Audit trails in clinical trial systems
7. Audit trails when the system is an AI or integration layer
8. Worked example: a reprocessed result
9. Inspector question list
10. Status and scope
11. Sources

Generate, protect, review: three duties that get conflated

Inspection findings about audit trails usually blur three different obligations. The first is to **generate** a trail: the system must record who did what to a record, when, and where required why. The second is to **protect** it: the trail must be complete, unalterable by the people it records, and retained as long as the data. The third is to **review** it: someone accountable must read the relevant parts of the trail, at a frequency that matches the risk, and act on what they find.

An audit trail, in the FDA's wording, is "a secure, computer-generated, time-stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record" (FDA, Data Integrity and Compliance With Drug CGMP, Q&A 1.c, December 2018). The EMA guideline on computerised systems in clinical trials uses almost the same definition. (A short glossary entry is at audit trail.)

A system can generate an excellent trail that nobody reviews; a quality unit can diligently review a trail an administrator could edit. Keeping the duties apart makes such gaps visible.

Duty	US anchor	EU GMP anchor	Clinical trials anchor	Typical failure
Generate	21 CFR 11.10(e)	Annex 11, clauses 9 and 12.4	EMA guideline 6.2.1; ICH E6(R3) 4.2.2	Trail disabled, or records events per page rather than per field
Protect	21 CFR 11.10(e); 21 CFR 211.68(b)	Annex 11, clauses 7.1, 7.2, 12	EMA guideline 6.2.1 and section on privileged access	Administrators can switch off or edit the trail; trail lost in migration
Review	FDA Q&A 7 and 8	Annex 11, clause 9 ("regularly reviewed")	EMA guideline 6.2.2; ICH E6(R3) 4.2.3	No documented review, or review of everything with no focus

Duty 1: what a useful audit trail contains

The regulatory minimum

US Part 11 requires "secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records", and states that "record changes shall not obscure previously recorded information" (21 CFR 11.10(e)). Two words carry weight. *Independently* means the trail is produced by the system, not typed by the user. *Obscure* means a change may never overwrite the prior value; the old value must remain readable.

EU GMP Annex 11 frames generation through risk: "consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated 'audit trail')" (Annex 11, clause 9). Clause 12.4 adds that systems "should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time."

Who, what, when, why, and the values

The clinical guidance spells out the fields most precisely. The EMA guideline says "the audit trail should show the initial entry and the changes (value - previous and current) specifying what was changed (field, data identifiers) by whom (username, role, organisation), when (date/timestamp) and, where applicable, why (reason for change)", and that audit trails "should capture any changes in data entry per field and not per page" (EMA/INS/GCP/112288/2023, section 6.2.1). The MHRA's GXP data integrity guidance (section 6.13) describes the same content as the "who, what, when and why" of an action.

Field	Why it matters	Source wording
User identity (and role)	Attributes the action to a person, not a shared account	Annex 11 12.4; EMA 6.2.1 "username, role, organisation"
Timestamp, with time zone	Orders events; detects back-dating	Part 11 11.10(e); MHRA 6.13 "time and time zone where applicable"; ICH E6(R3) 4.2.2(d) suggests UTC
Record and field identifier	Locates the change at data-point level	EMA 6.2.1 "per field and not per page"
Previous and new value	Shows what the record said before	Part 11 "shall not obscure"; EMA "value - previous and current"
Action type (create, modify, delete, sign, reprocess)	Distinguishes data changes from workflow events	ICH E6(R3) 4.2.2(a)(iii) "workflow actions"
Reason for change	Lets a reviewer judge whether the change was justified	Annex 11 clause 9; MHRA 6.13

Record-level and system-level events

The FDA distinguishes trails "that track creation, modification, or deletion of data (such as processing parameters and results)" from trails "that track actions at the record or system level (such as attempts to access the system or rename or delete a file)" (FDA Q&A 1.c). Its example: the trail for an HPLC run "should include the user name, date/time of the run, the integration parameters used, and details of a reprocessing, if

any", with "change justification for the reprocessing". It also expects aborted or incomplete injections to be "captured in audit trails" and "investigated and justified" (Q&A 12). ICH E6(R3) asks that systems "maintain logs of user account creation, changes to user roles and permissions and user access" (4.2.2(a)(i)).

Reason for change and old/new values

A reason such as "correction" or "per SOP" fills the field without explaining anything. A controlled list of reasons with an "other, specify" option, plus validation that rejects empty entries on critical fields, helps.

Some systems log that a field changed without storing the previous value, or keep it in a history table unlinked from the audit view. The test: from the audit trail alone, can a reviewer reconstruct the record as it stood at any earlier time? If not, previously recorded information has, in practice, been obscured. That is the same property as reproducing a past state of any record.

ICH E6(R3) adds a related expectation for clinical data: corrections "should be attributed to the person or computerised system making the correction, justified and supported by source records around the time of original entry and performed in a timely manner" (4.2.4). Note "or computerised system": automated corrections need attribution too.

Duty 2: protecting the trail from the people it records

A trail is evidence about the people who use the system, so those people must not control it.

No switching off, or a record when it happens. The MHRA says "users should not be able to amend or switch off the audit trail. Where a system administrator amends, or switches off the audit trail a record of that action should be retained" (MHRA 6.13). The EMA guideline says it "should not be possible for 'normal' users to deactivate them", that deactivation by admin users should "automatically create an entry into a log file", and that entries "should be protected against change, deletion, and access modification" (6.2.1). ICH E6(R3) allows modification only "in rare circumstances (e.g., when a participant's personal information is inadvertently included in the data) and only if a log of such action and justification is maintained" (4.2.2(b)).

Independence of privileged users. The EMA guideline notes that admin users can change the system time, deactivate audit trails and make "changes to data that are not captured in the audit trail [e.g. backend table changes in the database(s)]", and concludes that users with privileged access "should be sufficiently independent from and not be involved in the management and conduct of the clinical trial". The same logic applies in a GMP laboratory.

Retention and backup. Part 11 requires audit trail documentation to be "retained for a period at least as long as that required for the subject electronic records" (11.10(e)). For drug CGMP, backup systems must assure "that backup data are exact and complete and that it is secure from alteration, inadvertent erasures, or loss" (21 CFR 211.68(b)). Annex 11 asks that the ability to restore backups be "checked during validation and monitored periodically" (clause 7.2).

Migration. The EMA guideline says "data, contextual information, and the audit trail should not be separated" when data are migrated. Annex 11 clause 4.8 requires migration validation to check that data "are not altered in value and/or meaning". A migration plan that moves current values and archives the trail as a PDF has

separated them.

Duty 3: review — scope, frequency, and who

Who reviews

The FDA compares audit trail review to "assessing cross-outs on paper when reviewing data" and says "personnel responsible for record review under CGMP should review the audit trails that capture changes to data associated with the record as they review the rest of the record" (FDA Q&A 7). Production and control records, including audit trails, must be reviewed and approved by the quality unit under § 211.192. The MHRA adds that reviewers "should have sufficient knowledge and system access to review relevant audit trails, raw data and metadata" (6.13).

How often

The FDA's answer has two branches (Q&A 8):

1. If the regulations specify a review frequency for the data, the audit trail follows it. Section 211.188(b) requires review after each significant step in manufacture, and § 211.22 requires data review before batch release.
2. Otherwise, set the frequency "using knowledge of your processes and risk assessment tools", evaluating "data criticality, control mechanisms, and impact on product quality". A footnote gives examples suitable for risk-based frequency: trails capturing "instrument operational status, instrument communication logs, and alert records".

What to review

Not everything. The MHRA states "it is not necessary for audit trail review to include every system activity (e.g. user log on/off, keystrokes etc.)" and that review "may be limited to those with GXP relevance", performed either as a list of relevant data or by "a validated 'exception reporting' process" that flags predetermined abnormal data or actions (MHRA 6.13).

A risk-based review design

The table below is an illustrative design, not a regulatory template. It assigns each class of event a review point and a rationale traceable to the guidance above.

Event class	Example	Review point	Reviewer	Rationale
Changes to reportable results	Re-integration of a chromatographic peak	With the record, before batch release	Second-person reviewer, then quality unit	FDA Q&A 8, first branch (§ 211.22, § 211.188(b))
Aborted, incomplete or deleted runs	Injection aborted mid-sequence	With the record	Second-person reviewer	FDA Q&A 12: investigate and justify
Method or configuration changes	Integration parameters in a processing method	Each change, plus periodic	System owner and QA	Annex 11 clause 10 change control

Event class	Example	Review point	Reviewer	Rationale
Audit trail or time-setting changes	Clock changed, trail paused	Every occurrence, via exception report	QA, independent of users	MHRA 6.13; EMA 6.2.1
Account and privilege changes	Analyst granted admin role	Periodic (for example monthly)	IT quality and QA	ICH E6(R3) 4.2.2(a)(i); Annex 11 clause 12
Instrument status and alerts	Communication-loss alerts	Risk-based periodic	System owner	FDA Q&A 8, footnote 13
Log-on and log-off	Successful logins	Not routinely; on investigation	—	MHRA 6.13: not every activity

Document the review itself: who reviewed which trail, for which record or period, what was found, and the disposition. An undocumented review cannot be shown to an inspector. The FDA also says your approach should ensure "the reliability of the review is proven", which in practice means testing that exception reports actually catch the events they are meant to catch.

Audit trails in clinical trial systems

Clinical systems carry additional expectations. The EMA guideline asks that audit trails be "visible at data-point level in the live system" and exportable "as a dynamic data file to allow for the identification of systematic patterns or concerns in data across trial participants, sites, etc." (6.2.1). It also warns that "information jeopardising the blinding" must not appear in audit trails accessible to blinded users.

On review, the guideline requires "procedures for risk-based trial specific audit trail reviews", focused on critical data, "proactive and ongoing" unless justified, and lists what review is for: missing data, signs of manipulation, outliers, "data entered at unexpected or inconsistent hours and dates", incorrect processing, unauthorised access, and device malfunction (6.2.2). It adds that investigators should be introduced to navigating the audit trail of their own data. ICH E6(R3), adopted on 6 January 2025, states that review of data, audit trails and metadata "should be a planned activity, and the extent and nature should be risk-based, adapted to the individual trial and adjusted based on experience during the trial" (4.2.3).

Audit trails when the system is an AI or integration layer

More regulated data now pass through layers that are not the system of record: interfaces that move results from instruments to a LIMS, extract jobs feeding analytics, and AI components that summarise or classify. The guidance quoted here does not address AI audit trails specifically, so what follows applies its principles by analogy.

- **Integration jobs are actors.** Annex 11 clause 5 expects systems exchanging data electronically to "include appropriate built-in checks for the correct and secure entry and processing of data". If an interface can create or modify GxP records, its actions need the same who, what, when and why as a human's, with the service identity recorded.

- **Extracts must be traceable.** The EMA guideline notes that extracts for reporting "do not necessarily need to contain the audit trail information", but "the database audit trail should capture the generation of data extracts and exports" (6.2.1).
- **Automated changes need attribution.** ICH E6(R3) 4.2.4 attributes corrections to "the person or computerised system making the correction". For an AI component that proposes or applies a value, a reconstructable record would include the input, the output, the model or configuration version, and the human who accepted or rejected it.
- **Custody across layers.** When a value crosses systems, the trail in each system covers only its own segment. Linking those segments is the chain of custody problem.

Worked example: a reprocessed result

Halden Therapeutics AG is a fictional company used for illustration.

A Halden QC analyst runs an assay on a stability sample. The first integration gives 94.1 % of label claim, below the 95.0 % specification. Forty minutes later the same analyst re-integrates the peak with a modified baseline and reports 95.6 %.

What the trail must show for this to be defensible:

Time (UTC)	User	Action	Old value	New value	Reason
09:12	analyst.k	Run acquired	—	Sequence S-114, injection 3	—
09:20	analyst.k	Result calculated	—	94.1 %	—
10:01	analyst.k	Processing method modified	Baseline: valley-to-valley	Baseline: manual	"Peak tailing, baseline drawn per SOP QC-117"
10:02	analyst.k	Result recalculated	94.1 %	95.6 %	Reprocessing

A reviewer reading only the report sees a pass. A reviewer reading the trail with the record, as the FDA's "cross-outs" analogy asks, sees a failing result turned into a passing one by a manual baseline, and asks whether SOP QC-117 permits that, whether the first result was investigated as out of specification, and whether the analyst shows a pattern of manual integrations near limits. An exception report for "manual integration within 2 % of a specification limit" brings the event forward without reading every log line.

Inspector question list

Questions an inspector can be expected to ask, each traceable to the texts above:

1. Which systems hold GxP records, and is the audit trail enabled on each? Show the risk assessment that decided this (Annex 11 clause 9).
2. Show the audit trail for this specific result. Can you reconstruct every earlier value? (Part 11 11.10(e))

3. Who can disable the audit trail, change system time, or edit data at database level? Show the log of each time that happened. (MHRA 6.13; EMA 6.2.1)
4. Do any users who generate data also hold administrator rights? (EMA guideline on privileged access)
5. What is your audit trail review procedure, who performs it, and at what frequency? Why that frequency? (FDA Q&A 7 and 8)
6. Show the documented review for this batch or this trial period, and what was done with the findings.
7. How do you know your exception reports catch what they are designed to catch?
8. How were audit trails retained through the last migration or system retirement? (Annex 11 clause 4.8; EMA guideline)
9. Are backups restorable, and when was restoration last tested? (Annex 11 clause 7.2; 21 CFR 211.68(b))
10. For clinical systems: can investigators see the audit trail for their own data, and is blinding protected in audit views? (EMA 6.2.1, 6.2.2)

Status and scope

Revised Annex 11. The Commission and PIC/S consulted on a revised Annex 11 and a new Annex 22 from 7 July to 7 October 2025. On 28 October 2026 the EudraLex Volume 4 page still lists the January 2011 Annex 11, the text cited here.

This article is educational and is not regulatory advice; apply it through your own quality system and the regulations that govern your products and jurisdictions. Reliable Context keeps a cited, dated source behind every value and keeps any past state reproducible, the same properties an audit trail is meant to evidence.

Sources

1. 21 CFR 11.10, Controls for closed systems (eCFR) — audit trail requirement, "shall not obscure", retention.
2. 21 CFR 211.68, Automatic, mechanical, and electronic equipment (eCFR) — controls over computer systems and backup data.
3. FDA, Data Integrity and Compliance With Drug CGMP: Questions and Answers, Guidance for Industry, December 2018 — audit trail definition, who reviews, review frequency, aborted runs.
4. EudraLex Volume 4, Annex 11: Computerised Systems (2011) — clauses 4.8, 5, 7, 9, 10, 12.4.
5. European Commission, EudraLex Volume 4 page — Annex 11 version in force, checked 28 October 2026.
6. PIC/S, Joint stakeholders consultation on the revision of Chapter 4, Annex 11 and new Annex 22, 7 July 2025 — consultation dates.
7. MHRA, 'GXP' Data Integrity Guidance and Definitions, Revision 1, March 2018 — section 6.13 on audit trail content, protection and review.
8. EMA, Guideline on computerised systems and electronic data in clinical trials, EMA/INS/GCP/112288/2023 — sections 6.2.1, 6.2.2, privileged access, migration.
9. ICH E6(R3) Guideline for Good Clinical Practice, adopted 6 January 2025 — sections 4.2.2-4.2.4 and glossary.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-integrity-and-compliance-drug-cgmp-questions-and-answers
2. https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-computerised-systems-and-electronic-data-clinical-trials_en.pdf
3. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/subpart-B/section-11.10
4. https://health.ec.europa.eu/system/files/2016-11/annex11_01-2011_en_0.pdf
5. https://database.ich.org/sites/default/files/ICH_E6%28R3%29_Step4_FinalGuideline_2025_0106.pdf
6. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-C/part-211/subpart-D/section-211.68
7. https://assets.publishing.service.gov.uk/media/5aa2b9ede5274a3e391e37f3/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf
8. https://picscheme.org/en/news/joint-stakeholders-consultation-on-the-revision-of-chapter-4
9. https://health.ec.europa.eu/medicinal-products/eudralex/eudralex-volume-4_en

THE PUBLISHER

About Reliable Context

Reliable Context is a system of record for organizations that fuse private and public information and must defend every value they act on.

The guarantees

One canonical record per real thing: duplicates resolve by rule, ambiguity is shown rather than hidden, and related organizations relate without ever being merged. A verbatim, cited source and an observation date sit behind every value. Unknowns are declared as not found, blocked or not applicable with a reason, never left as an empty cell. Any past state of the record is reproducible, together with what changed since.

Where it runs

It runs inside the customer's perimeter, one database per organization. Permitted sources, model routing, reader clearance and retention are set as the customer's own policies, and every value is exportable with its chain of custody for an auditor or regulator.

What it is not

It is not a vector database or a RAG framework, not a data catalog, MDM or data-quality suite, not a CRM or data-enrichment vendor, and not a chatbot or AI assistant. Where a reader needs one of those, the honest answer is to say so and point them there.

Visit

See Reliable Context.

Reliable Context is in production use in two sectors; more than six thousand of its identity decisions were made by rule and none has been reversed. Articles published here explain general practice, cite their primary and academic sources, and name the jurisdiction of any regulatory rule they describe. They are not legal, regulatory or compliance advice for a specific organization, and requirements change.

Website: https://reliablecontext.com

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.