Reliable Context

RELIABLE CONTEXT / RESEARCH & PRACTICAL GUIDANCE

ICH E6(R3) Data Governance: Trial Data Traceability

> 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 · ich e6 r3 · ich e6(r3) data governance · good clinical practice data integrity · gcp electronic source data · ich e6 r3 changes

Original article: https://reliablecontext.com/articles/ich-e6-r3-data-governance-clinical-trial-data-traceability



In this article

1. What this article covers
2. Status and dates
3. What changed from R2 to R3, as far as data is concerned
4. Principles that frame section 4
5. Data governance: who is responsible for what
6. The data life cycle, element by element
7. Computerised systems and audit trails
8. Source records and certified copies
9. A worked example: one value, traced
10. Relation to other guidance
11. Checklist for trial data systems
12. Summary
13. Sources

What this article covers

ICH E6(R3) is the third revision of the International Council for Harmonisation (ICH) guideline for Good Clinical Practice (GCP). It sets the international ethical and scientific quality standard that regulators in ICH regions apply to interventional clinical trials. Most commentary on the revision concentrates on risk-based quality management and decentralised elements. This article reads a narrower part of it, the new section 4, "Data Governance – Investigator and Sponsor", as if it were a specification for a trial data system. The question throughout is simple: when an inspector picks one value in an analysis data set, what must exist for anyone to trace it back to the observation it came from?

The article is educational. It describes what the guideline text says and how its provisions can be read together. It is not legal or regulatory advice, and the binding effect of the guideline depends on the jurisdiction that adopts it.

Status and dates

The ICH Step 4 document for the Principles and Annex 1 is titled "Guideline for Good Clinical Practice E6(R3)" and was endorsed by the ICH regulatory members on 6 January 2025. Regional adoption followed on different dates:

Jurisdiction	Instrument	Status as read on 28 October 2026
European Union	Principles and Annex 1	In effect since 23 July 2025, per the EMA guideline page
European Union	Annex 2	ICH adoption 3 June 2026, CHMP adoption 25 June 2026, coming into effect 15 January 2027 (EMA); EMA has also published a consolidated version of the principles, Annex 1 and Annex 2

Jurisdiction	Instrument	Status as read on 28 October 2026
United States	E6(R3) Good Clinical Practice	Final guidance dated September 2025, docket FDA-2023-D-1955 (FDA)
United States	E6(R3) Annex 2	Still a draft guidance dated December 2024, docket FDA-2024-D-5601, "Not for implementation"; no final FDA version had been posted (FDA)

The section numbers cited below are from the January 2025 Step 4 text of the Principles and Annex 1. Annex 2 is not cited section by section here.

What changed from R2 to R3, as far as data is concerned

E6(R2) was an addendum integrated into the 1996 guideline; its document history lists the changed paragraphs, including the computerised-system provisions in section 5.5.3. R2 spoke of "source documents" and set out "essential documents for the conduct of a clinical trial" in its section 8. R3 is restructured. It is composed of Principles and Annexes, and the Principles are written to "remain relevant as technological and methodological advances occur" (E6(R3), Introduction).

Three changes matter most for data teams:

1. **Vocabulary moves from documents to records and data.** R3 defines *source records* as "original documents or data (which includes relevant metadata) or certified copies of the original documents or data, irrespective of the media used", and lists ePRO data and data from wearables and sensors among them (E6(R3), Glossary). *Essential records* replace essential documents and are defined as "documents and data (and relevant metadata), in any format".
2. **Metadata is part of the record.** The glossary defines metadata as "the contextual information required to understand a given data element", and "relevant metadata" as those needed to allow the appropriate evaluation of trial conduct. Audit trails are defined as metadata records.
3. **A dedicated data governance section.** Section 4 brings data life cycle, audit trails, computerised systems, security, validation and user management into one place and assigns them to the "responsible party", meaning the investigator or the sponsor depending on who deploys the system.

Principles that frame section 4

Two of the eleven principles carry most of the weight for data.

Principle 7 is proportionality: trial processes "should be implemented in a way that is proportionate to the risks to participants and to the importance of the data collected" (E6(R3), Principle 7). Principle 9 is reliability. It says that computerised systems should be fit for purpose, "through risk-based validation, if appropriate" (9.3), and that records management should help ensure "that record integrity and traceability are maintained" (9.4). Principle 9.5 requires essential records to be retained securely and made available to regulators, monitors, auditors and ethics committees on request.

The consequence is that R3 rarely says "always". It says "proportionate", "based on risk" and "data of higher criticality". A data system that treats every field identically is not wrong, but it cannot show the risk reasoning that R3 asks the responsible party to document.

Data governance: who is responsible for what

Section 4 opens by stating its purpose: guidance to investigators and sponsors "on appropriate management of data integrity, traceability and security". It names four key processes that "should address the full data life cycle with a focus on the criticality of the data" (E6(R3), section 4):

- (a) protection of the confidentiality of participants' data;
- (b) management of computerised systems so that they are fit for purpose and used appropriately;
- (c) safeguarding essential elements such as randomisation, dose adjustments and blinding;
- (d) support for key decisions such as data finalisation before analysis, unblinding and allocation to analysis data sets.

The split of duties is set out in sections 2 and 3. The investigator "should maintain adequate source records", and those records "should be attributable, legible, contemporaneous, original, accurate and complete"; changes "should be traceable, should not obscure the original entry and should be explained if necessary (via an audit trail)" (2.12.2). The investigator must also define, before the trial starts, what counts as a source record, the methods of data capture and their location. Data reported to the sponsor "should be consistent with the source records or the discrepancies explained" (2.12.6).

The sponsor "should ensure the integrity and confidentiality of data generated and managed" (3.16.1(a)), pre-specify the data to be collected in the protocol, and, where necessary, describe the flow in a data flow diagram in a protocol-related document such as a data management plan (3.16.1(c)). The sponsor "should not make changes to data entered by the investigator or trial participants unless justified, agreed upon in advance by the investigator and documented" (3.16.1(i)).

Duty	Investigator (section 2)	Sponsor (section 3)
Define source	What is a source record, capture method, location (2.12.2)	Pre-specify data and collection method; data flow diagram (3.16.1(c))
Integrity of entries	ALCOA-style attributes of source records (2.12.2)	Integrity for the full data life cycle (3.16.1(e))
Corrections	Traceable, not obscuring original (2.12.6)	Only with justification and investigator agreement (3.16.1(i))
Systems	Secure, attributable access for systems it deploys (2.12.10)	Data acquisition tools validated before use (3.16.1(d))

The data life cycle, element by element

Section 4.2 says "procedures should be in place to cover the full data life cycle" and then lists eight elements. Read as requirements on a system, they look like this.

Section	Element	What the text asks	What a system has to be able to show
4.2.1	Data capture	Verification of transcription scaled to criticality; captured data "accompanied by relevant metadata"; risk-based automated validation checks, controlled and documented	Which values were transcribed versus directly captured; which edit checks fired
4.2.2	Metadata, including audit trails	Logs of account creation, role and permission changes and access; initial entry and changes or deletions documented with reason where appropriate; workflow actions recorded; audit trails not disabled; unambiguous timestamps (e.g. UTC)	A complete, interpretable change history per data point and per user
4.2.3	Review of data and metadata	Planned, risk-based review of data, audit trails and metadata	Evidence that review happened and what it found
4.2.4	Data corrections	Corrections attributed, justified, supported by source records "around the time of original entry", timely	The correction, who made it, why, and the supporting source
4.2.5	Transfer, exchange, migration	Validated or reconciled transfers; documented to ensure traceability	Reconciliation results between systems, including metadata
4.2.6	Finalisation before analysis	Pre-specified, documented finalisation; data extraction per the statistical analysis plan	Which data were in the locked set and how they were derived
4.2.7	Retention and access	Retrievable, readable, protected from unauthorised access and alteration for the retention period	Readable archives with their metadata
4.2.8	Destruction	Permitted when no longer required by applicable regulatory requirements	A record of what was destroyed and on what authority

Two provisions in 4.2.2 are unusually specific. First, audit trails "should not be modified except 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)). That is a recognition that privacy and immutability can conflict, with a stated resolution: the redaction itself becomes an audited event. Second, automatic date and time capture must be "unambiguous (e.g., coordinated universal time (UTC))" (4.2.2(d)). A timestamp without a time zone is ambiguous by construction.

Computerised systems and audit trails

Section 4.3 applies to every computerised system used in the trial, whoever developed it. The responsible party "is responsible for the validation status of the system throughout its life cycle", and the validation approach "should be based on a risk assessment that considers the intended use of the system" and the importance of the data it holds (4.3.4(a)). Validation covers standard functionality and protocol-specific

configuration, including "automated data entry checks and calculations", and "interfaces between systems should also be defined and validated" (4.3.4(e)). Subsequent changes are validated based on risk and "should consider both previously collected and new data" (4.3.4(c)).

User management (4.3.8) ties access to attributability: access controls exist "to limit system access to authorised users and to ensure attributability to an individual", permissions are revoked when no longer needed, and records of authorised users must include role changes and "time of access permission being granted (e.g., time stamp)".

The R3 glossary definition of an audit trail is worth quoting in full because it is the test any implementation must meet: the audit trail "should show activities, initial entry and changes to data fields or records, by whom, when and, where applicable, why. In computerised systems, the audit trail should be secure, computer-generated and time stamped" (E6(R3), Glossary). The site glossary entry on the audit trail discusses the same who, what, when and why structure outside the clinical setting.

The EMA's guideline on computerised systems and electronic data in clinical trials (EMA/INS/GCP/112288/2023, final version adopted by the GCP Inspectors Working Group on 7 March 2023) is more operational. In its section 6.2.1 it expects that "it should not be possible for 'normal' users to deactivate" audit trails, that audit trails be "visible at data-point level in the live system", that it be possible "to export the entire audit trail as a dynamic data file", and that the trail record the value "previous and current", the field and data identifiers, the user's "username, role, organisation", the timestamp and the reason for change. It adds that changes should be captured "per field and not per page". Its section 6.2.2 describes risk-based audit trail review aimed at, among other things, data "entered at unexpected or inconsistent hours and dates" and unauthorised access.

Source records and certified copies

A *certified copy* in R3 is "a copy (irrespective of the type of media used) of the original record that has been verified (i.e., by a dated signature or by generation through a validated process) to have the same information as the original, including relevant metadata, where applicable" (E6(R3), Glossary). Because the source-record definition includes certified copies, a properly made copy can stand in for an original.

The EMA guideline explains why "same information" is harder than it sounds. Its section 6.5 distinguishes static content (a PDF), dynamic content (a worksheet with calculations) and content produced by an interpreter (a web page rendered by a browser). For interpreted content, it notes that window size, browser type, operating system and software dependencies "can influence the structure and content displayed" (EMA guideline, 6.5). A screenshot of an eCRF page is therefore not automatically a certified copy of the eCRF record: it may lose the audit trail and any values that only appear on interaction.

A worked example: one value, traced

The example uses a fictional sponsor, Halden Therapeutics AG, running a fictional phase II trial. The value under inspection is a systolic blood pressure of 142 mmHg for participant 0417 at visit 3, which appears in the locked analysis data set.

Step	Record	Evidence that R3 points to
1. Observation	Site nurse measures 142 mmHg with a validated automated cuff	Source defined before the trial as the device printout, filed in the participant chart (2.12.2)
2. Transcription	Nurse enters 124 in the eCRF on 2026-03-04 09:12 UTC	Audit trail: initial entry, user, role, timestamp (4.2.2(a)(ii), (d))
3. Query	Edit check flags a discrepancy against the device feed; data manager raises a query	Validation check documented (4.2.1(c)); workflow action recorded (4.2.2(a)(iii))
4. Correction	Investigator changes 124 to 142 on 2026-03-05, reason "transcription error, see device printout"	Correction attributed, justified, supported by source (4.2.4); original value still visible (2.12.6)
5. Transfer	EDC export to the sponsor's statistical environment	Reconciliation of record counts and values, including metadata (4.2.5)
6. Lock	Value included in the final data set under the statistical analysis plan	Documented finalisation and extraction (4.2.6)

An inspector can now walk backwards: from the analysis value to the export, from the export to the eCRF field, from the field's audit trail to the corrected entry, and from the correction to the printout. If any link is missing, for example if the export dropped the audit trail and no reconciliation exists, the value may be correct and still not be traceable. R3 treats those as different things.

The same pattern applies outside trials. Any value a regulated organisation acts on needs a path back to an identified source, with each transformation recorded; the site's sector notes for pharma describe that requirement from the data owner's side.

Relation to other guidance

R3 sits alongside, not above, other instruments:

- **EU.** The EMA computerised systems guideline elaborates many of the same points and expands ALCOA to "ALCOA++": attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, available when needed and traceable (EMA guideline, abbreviations and 4.5).
- **United States.** FDA has issued E6(R3) as final guidance (FDA). Separately, 21 CFR Part 11 is a regulation, and for closed systems it requires "secure, computer-generated, time-stamped audit trails" whose record changes "shall not obscure previously recorded information" (21 CFR 11.10(e)). The language closely matches R3's audit trail definition.
- **Trial registration.** Principle 9.6 links transparency to "timely registration on publicly accessible and recognised databases". Registry identifiers such as the NCT number are what tie a trial's records to its public registration.

Checklist for trial data systems

The following questions restate section 4 as checks that a sponsor, CRO or site can apply to any system that holds trial data. Each is a reading of the cited provision, not an additional requirement.

1. Is it documented, before first participant in, what the source record is for each critical data element, and where it lives? (2.12.2, 3.16.1(c))
2. Does every captured value carry the metadata needed to evaluate it, including whether it was transcribed or directly captured? (4.2.1(b))
3. Does the audit trail record initial entry, every change and deletion, the user, the time in an unambiguous zone, and the reason where appropriate? (4.2.2(a), (d))
4. Can ordinary users disable the audit trail? Is any modification of the trail itself logged and justified? (4.2.2(b))
5. Is audit trail and metadata review planned, risk-based and documented? (4.2.3)
6. Are corrections attributed, justified and tied to the source record? (4.2.4)
7. Is every transfer between systems validated or reconciled, metadata included? (4.2.5)
8. Is the locked data set reproducible from documented extraction steps? (4.2.6)
9. Are archives readable for the full retention period, with metadata, and protected from alteration? (4.2.7)
10. Are user accounts, role changes and access grant times recorded and periodically reviewed? (4.3.8)
11. Is validation scoped by intended use and criticality, and does it cover configuration, calculations and interfaces? (4.3.4)
12. Are copies that replace originals verified, including their metadata and, for dynamic content, their dynamic behaviour? (Glossary; EMA 6.5)

Summary

ICH E6(R3) section 4 does not prescribe a technology. It describes properties: every value attributable, every change visible, every transfer reconciled, every copy verified, and every review proportionate to what the data is used for. Read that way, it is a specification for traceability that a reviewer can check value by value. Reliable Context is built for organisations that need to defend individual values in this way.

Sources

1. ICH, *Guideline for Good Clinical Practice E6(R3)*, Step 4 final version, adopted 6 January 2025. https://database.ich.org/sites/default/files/ICH_E6(R3)_Step4_FinalGuideline_2025_0106.pdf
2. ICH, *E6(R2) Integrated Addendum to ICH E6(R1): Guideline for Good Clinical Practice*, 9 November 2016. https://database.ich.org/sites/default/files/E6_R2_Addendum.pdf
3. European Medicines Agency, *ICH E6 Good clinical practice – Scientific guideline* (adoption and effective dates). https://www.ema.europa.eu/en/ich-e6-good-clinical-practice-scientific-guideline
4. U.S. Food and Drug Administration, *E6(R3) Good Clinical Practice (GCP)*, final guidance, September 2025. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/e6r3-good-clinical-practice-gcp
5. European Medicines Agency, GCP Inspectors Working Group, *Guideline on computerised systems and electronic data in clinical trials*, EMA/INS/GCP/112288/2023. https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-computerised-systems-and-electronic-data-clinical-trials_en.pdf

6. Electronic Code of Federal Regulations, 21 CFR 11.10, Controls for closed systems. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/subpart-B/section-11.10
7. U.S. Food and Drug Administration, *E6(R3) Good Clinical Practice: Annex 2*, draft guidance, December 2024, docket FDA-2024-D-5601. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/e6r3-good-clinical-practice-annex-2

Source links

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

1. https://database.ich.org/sites/default/files/ICH_E6%28R3%29_Step4_FinalGuideline_2025_0106.pdf
2. https://www.ema.europa.eu/en/ich-e6-good-clinical-practice-scientific-guideline
3. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/e6r3-good-clinical-practice-gcp
4. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/e6r3-good-clinical-practice-annex-2
5. https://database.ich.org/sites/default/files/E6_R2_Addendum.pdf
6. https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-computerised-systems-and-electronic-data-clinical-trials_en.pdf
7. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/subpart-B/section-11.10

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.