Reliable Context

RELIABLE CONTEXT / RESEARCH & PRACTICAL GUIDANCE

Data Integrity Guidance Compared: FDA, EMA, MHRA, PIC/S, WHO

> 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 · data integrity guidance fda vs mhra · pic/s data integrity · mhra gxp data integrity guidance · who data integrity guideline · gxp data integrity regulations compared

Original article: https://reliablecontext.com/articles/data-integrity-guidance-compared-fda-ema-mhra-pics-who



In this article

1. Why five documents describe one problem
2. FDA: Data Integrity and Compliance With Drug CGMP, Questions and Answers (United States)
3. MHRA: GxP Data Integrity Guidance and Definitions (United Kingdom)
4. PIC/S PI 041-1 (inspectorates)
5. WHO TRS 1033, Annex 4: Guideline on data integrity
6. EMA and EU GMP: Annex 11 and the clinical-trial guideline (European Union)
7. Comparison table: definitions, audit trail, review, governance, retention
8. Where they differ and how to build once
9. Contract-manufacturer questionnaire

Why five documents describe one problem

Data integrity, in regulated medicines work, is the property that a record can be trusted to show what actually happened, now and years later. A global quality organisation meets guidance on it from five bodies: the US Food and Drug Administration (FDA), the UK Medicines and Healthcare products Regulatory Agency (MHRA), the Pharmaceutical Inspection Co-operation Scheme (PIC/S, a network of inspectorates), the World Health Organization (WHO), and the European Union, where the European Medicines Agency (EMA) and the European Commission publish the relevant texts. The documents overlap heavily; the MHRA calls its guidance "a UK companion document to PIC/S, WHO, OECD … and EMA guidelines" (MHRA guidance, §2.1). They still differ in scope, in the attributes they list, in how precisely they state when audit trails must be reviewed, and in what they say about retention.

This article sets six texts side by side (one each from FDA, MHRA, PIC/S and WHO, two from the EU), checked against the documents on 28 October 2026. Where a document says nothing on a point, the table says "silent". **GxP** is the umbrella term for the "good practice" regimes (manufacturing, clinical, laboratory, distribution, pharmacovigilance). An **audit trail** is metadata that records the creation, change or deletion of a record so the history can be reconstructed (see the audit trail glossary entry). This is an educational comparison across jurisdictions (United States, United Kingdom, European Union, and the international PIC/S and WHO frameworks). It is not legal or regulatory advice.

FDA: Data Integrity and Compliance With Drug CGMP, Questions and Answers (United States)

FDA issued this final guidance in December 2018 (docket FDA-2018-D-3984); on 28 October 2026 its page still showed "content current as of 12/13/2018" with no notice that it had been superseded (FDA guidance page). It covers current good manufacturing practice (CGMP) for drugs, including biologics, under 21 CFR parts 210, 211 and 212. Like all FDA guidance, it is nonbinding: "should" means recommended, not required, unless a regulation is cited (FDA Q&A, Introduction).

Q1 defines data integrity as "the completeness, consistency, and accuracy of data", and says that such data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA). Q1 also defines an audit trail as "a secure, computer-generated, time-stamped electronic record" that allows the course of events to be reconstructed, and gives an HPLC run as its example (FDA Q&A, Q1). The Q&A is the most precise of the six on review frequency. Q8 says that where a CGMP regulation sets the review frequency for the underlying data, the audit trail is reviewed at the same frequency. The examples are review after each significant manufacturing step under § 211.188(b) and data review before batch release under § 211.22. Where no frequency is set, the firm decides using risk assessment. Q7 assigns audit-trail review to the people who review the rest of the record, and compares it to checking cross-outs on paper (FDA Q&A, Q7-Q8).

MHRA: GxP Data Integrity Guidance and Definitions (United Kingdom)

The MHRA published "Revision 1: March 2018" on 9 March 2018. The GOV.UK page was last updated on 27 September 2021, when a section on good laboratory practice was added (MHRA GOV.UK page). Its scope is the widest: GLP, GCP, GMP, GDP and pharmacovigilance. It presents itself as clarifying "the UK regulatory interpretation of existing requirements" (MHRA guidance, §2).

Section 6.4 defines data integrity as "the degree to which data are complete, consistent, accurate, trustworthy, reliable" and maintained so throughout the data lifecycle. Section 3.10 deals with the acronym question directly. The guidance uses ALCOA but says there is "no difference in expectations" from ALCOA+, because governance measures should in any case make data complete, consistent, enduring and available. Its ALCOA list in §6.1 reads "legible and permanent", which folds durability into L. On audit trails, §6.13 sets out a risk-based approach. Audit trails that risk assessment shows are needed should be switched on. Review need not cover "every system activity (e.g. user log on/off, keystrokes etc.)". Review can use an "exception report", which the guidance defines as a validated search that flags predetermined abnormal data or actions. Section 6.15 asks that a documented data review include "a positive statement regarding whether issues were found or not" (MHRA guidance, §3.10, §6.4, §6.13, §6.15).

PIC/S PI 041-1 (inspectorates)

PIC/S adopted PI 041-1, *Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments*, on 1 June 2021, and it entered into force on 1 July 2021. It is written for GMP and GDP inspectors, covers both on-site and remote inspections, and states plainly that it "is not mandatory or enforceable under law" (PIC/S PI 041-1, §1, §3.7, §4). Its definition of data integrity in §2.5 is the MHRA wording, quoted with a footnote to the MHRA document. PIC/S lists the full nine attributes (ALCOA plus complete, consistent, enduring and available) in §2.3 and §7.4.

PI 041-1 is the most operational of the six on audit trails. Under §9.6, audit-trail functions should be "enabled and locked at all times". Critical audit trails should be reviewed with the other records of an operation before that operation is closed out, for example before batch release, by the originating department and verified by the quality unit where needed. Non-critical audit trails can be reviewed "at a pre-defined frequency" during

system reviews. Under §9.8, the frequency, roles and responsibilities of review follow a risk assessment, and a detailed SOP (standard operating procedure) should say what reviewers look for. The quality unit should also run a programme of audit-trail reviews within self-inspection, with selection that is both "random" and "targeted" (PIC/S PI 041-1, §9.6, §9.8).

WHO TRS 1033, Annex 4: Guideline on data integrity

WHO published the guideline as Annex 4 to Technical Report Series No. 1033 (2021). It replaces the 2016 guidance on good data and record management practices (TRS 996, Annex 5), covers GxP for medical products, and applies to paper, electronic and hybrid systems (WHO TRS 1033 Annex 4, §1-2).

The WHO glossary has no separate entry for "data integrity". It defines ALCOA+, data governance and data integrity risk assessment instead. Its definition of data governance also differs from PIC/S in one word: the arrangements provide assurance of data *quality*, where PIC/S says *integrity*. The audit-trail definition matches the MHRA's word for word, including the "who, what, when and why" of an action. WHO adds two expectations stated less clearly elsewhere. Audit trails should be enabled when software is installed, with "periodic verification" that they stay enabled (§11.11). Backups should be periodically restored and checked for completeness (§11.19). On review frequency, §12.3 names the factors (system criticality and category of audit-trail information, such as batch-specific, administrative or system activity) but sets no interval (WHO TRS 1033 Annex 4, §3, §11-12).

EMA and EU GMP: Annex 11 and the clinical-trial guideline (European Union)

In the European Union, two documents serve different regimes.

EudraLex Volume 4, Annex 11 (Computerised Systems) is revision 1, which came into operation on 30 June 2011. It is a GMP text for computerised systems, not a data integrity guideline, with no definition of data integrity and no ALCOA list. On audit trails, §9 is brief. Building in an audit trail of "all GMP-relevant changes and deletions" is to be considered "based on a risk assessment"; a reason must be recorded for changes; and audit trails "need to be available … and regularly reviewed". On retention, §7.1 requires that access to data be ensured throughout the retention period (EU GMP Annex 11). The retention periods themselves are in Chapter 4. Batch documentation is kept for one year after the batch expires or at least five years after certification by the Qualified Person, whichever is longer, and critical raw data supporting the marketing authorisation is kept while the authorisation remains in force (EU GMP Chapter 4, §4.10-4.12).

EMA Guideline on computerised systems and electronic data in clinical trials (EMA/INS/GCP/112288/2023) is dated 9 March 2023. The GCP Inspectors Working Group adopted it on 7 March 2023, and it took effect six months after publication (EMA guideline, cover page). Its attribute list is the longest of the six: ALCOA++, which is ALCOA+ with "available when needed" and "traceable" added. Section 4.1 says data integrity "is achieved when" data are collected, accessed and maintained securely so as to fulfil those ALCOA++ attributes. Its audit-trail definition is close to the FDA's. Section 6.2.1 asks for audit trails visible at data-point level and exportable "as a dynamic data file". Section 6.2.2 expects proactive, ongoing, risk-based review "unless justified", focused on critical data, and allows technology to help review large

datasets (EMA guideline, §4.1, §4.5, §6.2). On archiving, §6.11 asks for an inventory of essential data with retention periods, and asks that those periods respect the data-protection principle of storage limitation. The governing period is set by law: Regulation (EU) No 536/2014, Article 58, requires the trial master file to be archived for at least 25 years after the end of the trial (Clinical Trials Regulation, Art. 58).

Revision status as of 28 October 2026. On 7 July 2025 the European Commission opened a consultation on three drafts: a revised Chapter 4, a revised Annex 11, and a new Annex 22 on artificial intelligence. The EMA GMDP Inspectors Working Group drafted them with PIC/S, and the consultation closed on 7 October 2025 (Commission consultation page). On 28 October 2026, the EudraLex Volume 4 page still listed Annex 11 as "revision January 2011" and Chapter 4 as "January 2011", and it listed no Annex 22 (EudraLex Volume 4). The 2011 texts therefore remain the published versions, and the drafts are not yet in force.

Comparison table: definitions, audit trail, review, governance, retention

Dimension	FDA Q&A (US, Dec 2018)	MHRA (UK, Mar 2018)	PIC/S PI 041-1 (Jul 2021)	WHO TRS 1033 Annex 4 (2021)	EU GMP Annex 11 (2011)	EMA CT guideline (2023)
Scope	Drug CGMP, parts 210, 211, 212	All GxP incl. GLP, GPvP	GMP and GDP inspections	GxP for medical products	GMP computerised systems	Clinical-trial computerised systems
Stated legal status	Nonbinding recommendations	UK interpretation of existing requirements	"Not mandatory or enforceable"	Guideline	Detailed GMP guideline under Directive 2001/83/EC Art. 47	GCP IWG guideline
Definition of data integrity	Completeness, consistency, accuracy	Complete, consistent, accurate, trustworthy, reliable, through lifecycle	MHRA wording, cited	Silent (no glossary entry)	Silent	"Achieved when" data fulfil ALCOA++
Attribute list	ALCOA (5)	ALCOA; "+" said to add nothing new	ALCOA+ (9)	ALCOA+ (9)	Silent	ALCOA++ (11)
Audit-trail definition	Secure, computer-generated, time-stamped record	Metadata; paper or electronic; "who, what, when and why"	Metadata permitting reconstruction	Same wording as MHRA	System-generated record of GMP-relevant changes and deletions	Close to FDA wording
Audit trail on and locked	Silent on switch-off	On where risk assessment requires; admin changes recorded	Enabled and locked at all times	Enabled from installation; periodic verification	Built in "based on a risk assessment"	Cannot be deactivated by normal users

Dimension	FDA Q&A (US, Dec 2018)	MHRA (UK, Mar 2018)	PIC/S PI 041-1 (Jul 2021)	WHO TRS 1033 Annex 4 (2021)	EU GMP Annex 11 (2011)	EMA CT guideline (2023)
Review frequency language	Same as data review where a rule sets it; else risk-based	Risk-based; exception reports allowed	Critical: before batch release; non-critical: pre-defined frequency	Risk factors named; no interval	"Regularly reviewed"	Proactive and ongoing unless justified
Governance	Executive management builds quality culture	Policy endorsed at highest level; senior management accountable	Data governance system within the PQS	Written data integrity policy; senior management accountable	Silent (risk management, personnel roles)	Ownership, training, reporting culture
Reporting to regulators	Silent (Q18 covers remediation)	Notify significant incidents	Escalate to authorities where necessary	Report significant lapses	Silent	Sponsor reports serious breaches, incl. data breaches, within seven days (Annex 1)
Retention wording	Keep with metadata for retention period; periods in § 211.180	Protect through retention; archive stays readable	At least GMP/GDP periods; identify data-centre locations	Periods in authorised procedures; restore-tested backups	Access ensured through retention period	Inventory; storage limitation; all submission regions

Column sources: FDA Q&A, MHRA guidance (§3.9 for notification), PIC/S PI 041-1 (§5, §8.10, §9.8), WHO TRS 1033 Annex 4 (§4, §11), Annex 11, EMA guideline. The US batch-record period is one year after the batch's expiration date (21 CFR 211.180(a)).

Where they differ and how to build once

Four differences are substantive; the rest is wording.

1. **Attribute count.** Five, nine or eleven attributes look like a conflict, but the MHRA says expectations do not change with the acronym. The EMA additions are implied elsewhere by "available" and by audit-trail requirements, so one internal standard written to ALCOA++ meets every list.
2. **Review timing.** FDA ties audit-trail review to the regulatory review points for the underlying data. PIC/S ties critical audit-trail review to the decision the data supports, such as batch release. In practice both mean: review before the data are relied on. WHO and Annex 11 give no interval, which leaves the firm to set and justify one. The EMA's "ongoing unless justified" is the strictest default.
3. **Scope of what is reviewed.** The MHRA excludes routine noise such as log-ons and keystrokes. The EMA asks for review of access logs where they matter, for example in systems holding unblinded data. A risk assessment that classifies audit-trail events by category, which WHO §12.3 also suggests, settles both positions.

4. **Retention periods.** None of the data integrity guidelines sets a period. Each refers to the underlying regulation, and those differ: one year after expiry in the US, the longer of one year after expiry or five years after certification for EU batch records, and 25 years for an EU trial master file. The EMA guideline adds that archives must meet the periods of every region where the data may be submitted. A retention schedule keyed to record class and destination market therefore beats one keyed to site.

Worked example. Halden Therapeutics AG (a fictional pharma company) releases an oral solid product in the US, the EU and the UK. Its contract laboratory runs assay testing on an HPLC data system. Halden writes one control set that meets all six documents:

- Audit trails are enabled and locked at installation, and a quarterly check confirms they remain enabled (WHO §11.11).
- Audit-trail events are classed as critical (reintegration, method edits, deleted injections) or non-critical (log-ons, report prints).
- Critical events are reviewed through a validated exception report before the certificate of analysis is signed, which places review ahead of batch release (FDA Q8, PIC/S §9.6, MHRA §6.13).
- Non-critical events are reviewed quarterly during system review, and the quality unit samples both random and targeted runs within self-inspection.
- Every review record states whether issues were found, as the MHRA asks, and is dated and signed.
- Retention is the longest applicable period for each record class, with the dynamic chromatography files archived in a readable format.

In batch L-0417 (fictional), an analyst reintegrates a peak, citing "baseline drift". The exception report flags it; Halden's reviewer compares original and reprocessed results and records "no issue found". One review answers all six texts, because each asks the same question about the same event.

Contract-manufacturer questionnaire

Each document places responsibility on the party relying on the data. WHO says contract givers are "ultimately responsible" for data integrity at their contract acceptors. PIC/S expects quality agreements to require contract acceptors to notify the contract giver of data integrity failures. The MHRA expects data ownership, governance and accessibility to be written into contracts. Annex 11 requires formal agreements with third parties. The EMA keeps "full responsibility" with sponsors and investigators even when tasks are delegated (WHO §2.3; PIC/S §10.3; MHRA §6.5; Annex 11 §3.1; EMA Annex 1). The questions below combine the six into one supplier audit:

1. Which data integrity guidance does your quality system reference, and which version and date?
2. Is there a written data integrity policy, and who in senior management owns it?
3. For each GxP system that produces our data, is the audit trail enabled, locked, and checked periodically to confirm it stays enabled? Can administrators disable it, and is that action logged?
4. How do you classify audit-trail events as critical or non-critical, and what is the review point for each class?
5. Do you use validated exception reports? Show a recent one and the review record, including its positive statement.

6. Do individual user accounts exist on every instrument, or is there a dated plan to replace shared or legacy logins?
7. Where are the data stored, including data-centre locations, and under which retention periods for each market we supply?
8. How are dynamic records (chromatography, spectra) archived, and when were backups last restored and verified?
9. What do you send us: summary reports or raw data with metadata? How can we reach the audit trail behind a reported result?
10. How quickly will you notify us of a data integrity failure, and is that written into the quality agreement?

For the wider context of how these duties sit in regulated life sciences, see the pharma sector page.

Source links

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

1. https://assets.publishing.service.gov.uk/media/5aa2b9ede5274a3e391e37f3/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf
2. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-integrity-and-compliance-drug-cgmp-questions-and-answers
3. https://www.fda.gov/media/119267/download
4. https://www.gov.uk/government/publications/guidance-on-gxp-data-integrity
5. https://picscheme.org/docview/4234
6. https://cdn.who.int/media/docs/default-source/medicines/norms-and-standards/guidelines/inspections/trs1033-annex4-guideline-on-data-integrity.pdf
7. https://health.ec.europa.eu/system/files/2016-11/annex11_01-2011_en_0.pdf
8. https://health.ec.europa.eu/system/files/2016-11/chapter4_01-2011_en_0.pdf
9. https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-computerised-systems-and-electronic-data-clinical-trials_en.pdf
10. https://eur-lex.europa.eu/eli/reg/2014/536/oj
11. https://health.ec.europa.eu/consultations/stakeholders-consultation-eudralex-volume-4-good-manufacturing-practice-guidelines-chapter-4-annex_en
12. https://health.ec.europa.eu/medicinal-products/eudralex/eudralex-volume-4_en
13. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-C/part-211/subpart-J/section-211.180

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.