Reliable Context

RELIABLE CONTEXT / RESEARCH & PRACTICAL GUIDANCE

21 CFR Part 11 Explained: Records, Signatures, Audit Trails

> 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 · 21 cfr part 11 · part 11 compliance · fda electronic records electronic signatures · 21 cfr 11.10 · part 11 audit trail requirements

Original article: https://reliablecontext.com/articles/21-cfr-part-11-explained-electronic-records-signatures



In this article

1. What Part 11 is
2. Scope: which records Part 11 reaches
3. Section-by-section table
4. Subpart B: controls for closed systems (11.10)
5. Open systems: 11.30
6. Signatures on records: 11.50 and 11.70
7. Subpart C: electronic signatures
8. What FDA's 2003 guidance changed, and what it did not
9. Current FDA guidance
10. Predicate rules: Part 11 never stands alone
11. Worked example: Halden Therapeutics AG (fictional)
12. Gap-assessment checklist
13. Sources

What Part 11 is

21 CFR Part 11 is the US Food and Drug Administration (FDA) regulation that sets the conditions under which FDA treats electronic records and electronic signatures as "trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper" (21 CFR 11.1(a)). It was published on 20 March 1997 (eCFR source note, 62 FR 13464) and took effect on 20 August 1997 (FDA 2003 guidance, p. 2). The jurisdiction here is US federal law as administered by FDA. This article is an educational reading of public texts, not legal advice.

Part 11 has three subparts and ten sections: Subpart A (11.1 to 11.3) sets scope and definitions, Subpart B (11.10 to 11.70) governs electronic records, and Subpart C (11.100 to 11.300) governs electronic signatures. Each clause can be read as a question about a record: can it be trusted, can it be attributed to a person, and can its history be reproduced?

Scope: which records Part 11 reaches

Section 11.1(b) applies Part 11 to electronic records "created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations", and to electronic records submitted to FDA under the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act. It does not apply to paper records transmitted electronically. Paragraphs 11.1(f) to (p) exclude records required only by certain food and animal-food rules (for example parts 112, 117, 121 and 507).

The obligation to keep a record always comes from elsewhere. FDA calls those underlying requirements **predicate rules**: requirements in the Act, the PHS Act and FDA regulations other than Part 11 (FDA 2003 guidance, p. 1), such as drug current good manufacturing practice (CGMP) in part 211 or investigational new drug rules in part 312.

Key definitions in 11.3

Section 11.3 defines:

- **Electronic record**: any combination of text, graphics, data, audio, pictorial or other information in digital form that is created, modified, maintained, archived, retrieved or distributed by a computer system.
- **Electronic signature**: "a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature."
- **Handwritten signature**: a scripted name or legal mark executed by hand, which may be applied to devices that capture it. FDA treats a stylus signature on a tablet as handwritten, not electronic (FDA clinical Q&A, Q25).
- **Closed system**: "an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system."
- **Open system**: an environment in which access is *not* controlled by those persons.

Read literally, the closed/open test turns on who controls access, not on where a server sits. A vendor-hosted application whose accounts the regulated company administers fits the closed-system wording; a portal whose accounts a third party administers fits the open-system wording.

What counts as a "Part 11 record"

FDA's 2003 guidance lists four categories (FDA 2003 guidance, pp. 5-6):

1. Records required by a predicate rule and kept electronically in place of paper.
2. Records required by a predicate rule, kept in both forms, where the electronic version is relied on to perform regulated activities.
3. Records submitted to FDA electronically under predicate rules.
4. Electronic signatures intended to be the equivalent of handwritten signatures, initials and other signings required by predicate rules.

Records no predicate rule requires are not Part 11 records. Where a computer prints paper records that meet the predicate rules and staff rely on the paper, FDA "would generally not consider persons to be 'using electronic records in lieu of paper records'" (p. 5). FDA recommends documenting, record by record, which version is relied on.

Section-by-section table

Section	What the text requires (paraphrased)	Question it lets a reviewer ask
11.1 Scope	Equivalence criteria; applies to records under any FDA records requirement and to submissions; systems open to FDA inspection	Is this record required by a predicate rule?
11.2 Implementation	Electronic records and signatures may replace paper if Part 11 is met; submissions limited to types in docket 92S-0251	Is the electronic version the one relied on?

Section	What the text requires (paraphrased)	Question it lets a reviewer ask
11.3 Definitions	Electronic record and signature, handwritten and digital signature, biometrics, closed and open system	Is the system closed or open?
11.10 Closed systems	Controls (a) to (k): validation, copies, retention, access, audit trails, sequencing, authority and device checks, training, accountability, documentation control	Can the record be trusted, attributed and reconstructed?
11.30 Open systems	11.10 controls as appropriate, plus measures such as encryption and digital signature standards	Is integrity protected until receipt?
11.50 Signature manifestations	Printed name, date and time, meaning, also on displays and printouts	Who signed, when, to say what?
11.70 Signature/record linking	Signatures cannot be excised, copied or transferred by ordinary means	Can this signature move to another record?
11.100 General requirements	Unique to one person; identity verified; certification to FDA	Is each signature tied to one verified person?
11.200 Components and controls	Two components if not biometric; session rules; misuse needs two or more people	Could one person sign as another?
11.300 ID codes and passwords	Uniqueness, periodic checks, loss management, transaction safeguards, device testing	Are credentials still controlled?

Subpart B: controls for closed systems (11.10)

Section 11.10 requires controls "designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine." The eleven controls fall into four groups.

Trust in the system. Validation "to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records" (a); operational checks enforcing permitted sequencing of steps (f); device checks on the validity of input sources (h); and documentation control, including change control that maintains an audit trail of systems documentation (k).

Attribution. Access limited to authorized individuals (d); authority checks on who can use the system, sign, alter a record or perform an operation (g); education, training and experience of people who develop, maintain or use the system (i); and written policies holding individuals accountable for actions under their electronic signatures, "in order to deter record and signature falsification" (j).

Availability. Accurate and complete copies in human-readable and electronic form for FDA (b), and protection of records for ready retrieval throughout the retention period (c).

Reconstruction. The audit trail in (e).

The 11.10(e) audit trail requirement

Section 11.10(e) contains four obligations:

1. The audit trail is **secure, computer-generated and time-stamped**. A manually typed change log does not fit that description.
2. It **independently** records "the date and time of operator entries and actions that create, modify, or delete electronic records".
3. "Record changes shall not obscure previously recorded information." FDA's data integrity guidance compares audit trail review to "assessing cross-outs on paper" (data integrity Q&A, Q7).
4. The trail is **retained at least as long as the subject records** and available for FDA review and copying.

An audit trail records actions on records; it does not show that a value is correct. FDA's 2024 clinical guidance says audit trail components "must include (1) the date and time the data element or information was entered or modified ..., (2) the individual making the change (e.g., user ID and user role), and (3) the old value and the new value", should include the reason for a change if applicable, and "should be protected from modification and from being disabled" (FDA clinical Q&A, Q12). Every keystroke need not be recorded, but deliberate actions such as save or submit should be (Q13). For drug CGMP, FDA says audit trails should be reviewed at the frequency the regulations set for the underlying data, or at a risk-based frequency where none is set (data integrity Q&A, Q8).

Open systems: 11.30

Section 11.30 requires protection of authenticity, integrity and, as appropriate, confidentiality "from the point of their creation to the point of their receipt".

Aspect	Closed system (11.10)	Open system (11.30)
Defining test (11.3)	Access controlled by those responsible for content	Access not controlled by them
Baseline controls	11.10(a) to (k)	11.10 controls, as appropriate
Additional measures named	None	Document encryption, digital signature standards
Protection window	While records are on the system	From creation to receipt

Signatures on records: 11.50 and 11.70

Section 11.50 requires each signed electronic record to show the printed name of the signer, the date and time of signing, and the meaning of the signature, "such as review, approval, responsibility, or authorship". These items must appear in any human-readable form, including displays and printouts (11.50(b)).

Section 11.70 requires electronic and handwritten signatures executed to electronic records to be linked to those records "to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means". An image of a signature pasted into a document is one example of a signature that could be copied by ordinary means.

Subpart C: electronic signatures

Section 11.100 requires that each electronic signature be unique to one individual and never reused or reassigned (a), and that the organization verify the individual's identity first (b). Part 11 names no verification method; FDA lists government-issued identification and strong credentials with multi-factor authentication among options (FDA clinical Q&A, Q26). Users must certify to FDA, in a handwritten-signed letter, that their electronic signatures are intended to be legally binding equivalents of handwritten signatures (c); one letter may cover a whole organization (Q29). Section 11.100 was amended in March 2023 (88 FR 13018).

Section 11.200 requires non-biometric signatures to use "at least two distinct identification components such as an identification code and password". Within one continuous session, the first signing uses all components and later ones at least one component only the individual can execute; otherwise every signing uses all components. Attempted misuse must require "collaboration of two or more individuals".

Section 11.300 adds controls for identification code and password signatures: unique combinations, periodic checks or revision such as password aging, loss management for tokens and cards, safeguards that report unauthorized attempts "in an immediate and urgent manner", and periodic testing of tokens and cards.

What FDA's 2003 guidance changed, and what it did not

"Part 11, Electronic Records; Electronic Signatures — Scope and Application" is dated August 2003 on its cover (PDF); FDA's page lists it as final, docket FDA-2003-D-0143, labelled September 2003 (FDA guidance page). It rests on three elements (p. 4):

- Part 11 is interpreted narrowly.
- FDA intends to exercise **enforcement discretion**, meaning it does not intend to take enforcement action, on the requirements for validation (11.10(a)), audit trails (11.10(e), (k)(2)), record retention (11.10(c)) and record copying (11.10(b)), and corresponding parts of 11.30.
- FDA will enforce all predicate rules.

Three points are often lost. The guidance states that "part 11 remains in effect" (p. 2). FDA said it would keep enforcing access limits, operational, authority and device checks, training, accountability policies, documentation controls, the matching open-system controls, and sections 11.50, 11.70, 11.100, 11.200 and 11.300 (p. 4). And discretion on audit trails leaves predicate-rule obligations on dates, sequencing and "ensuring that changes to records do not obscure previous entries" untouched (p. 6). In each discretion area FDA recommends a "justified and documented risk assessment".

Systems operational before 20 August 1997 received broader discretion only if they met predicate rules before and after that date and were documented as fit for intended use (p. 7). A footnote says FDA does not expect a signer's local time across time zones, but documentation should explain the time zone reference (p. 3, fn. 5).

FDA said it anticipated rulemaking to revise Part 11 (p. 2). In the current eCFR, sections 11.10 to 11.70, 11.200 and 11.300 still carry only the 1997 source citation; later amendments touch the scope exclusions in 11.1 and section 11.100 (eCFR Part 11). The 11.100 change, a March 2023 technical amendment, only updated the address for paper certifications and added an electronic submission option; FDA described it as "nonsubstantive" (88 FR 13018).

Current FDA guidance

Clinical investigations. "Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations: Questions and Answers" is final, dated October 2024, docket FDA-2017-D-1105 (FDA guidance page). Its 29 questions "expand upon" the 2003 guidance; FDA "continues to apply a narrow and practical interpretation" of Part 11, while noting that audit trails, automated time stamps and complete copies are now "standard components of many electronic systems" (PDF, pp. 2-3). It states that Part 11 applies to required electronic records at non-US sites under an IND, IDE or INAD (Q2) and that FDA does not certify electronic signature systems (Q28).

Drug CGMP. "Data Integrity and Compliance With Drug CGMP: Questions and Answers" is final, dated December 2018 (FDA guidance page). It defines data integrity as completeness, consistency and accuracy, with data that are attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA). It explains why shared logins fail the attribution requirements of parts 211 and 212, and states that saving only the final result of reprocessed chromatography is not acceptable (PDF, Q1, Q5, Q14). Both guidances are nonbinding.

Predicate rules: Part 11 never stands alone

Part 11 says how an electronic record is controlled; the predicate rule says which record must exist and for how long. For a drug manufacturer, 21 CFR 211.68(b) requires that record changes be made only by authorized personnel and that backups be kept; 211.180(a) keeps batch records at least one year after batch expiration; and 211.194(a)(8) requires a second person's initials or signature on reviewed laboratory records. For a clinical investigator, 21 CFR 312.62(c) sets retention at two years after approval for the indication, or two years after the investigation is discontinued and FDA notified. A retention schedule naming the predicate rule for each record type connects the two layers.

Worked example: Halden Therapeutics AG (fictional)

Halden Therapeutics AG is fictional. It manufactures a sterile injectable for the US market, so its quality control (QC) laboratory records fall under part 211. Its chromatography data system (CDS) is administered by Halden's own staff, a closed system under 11.3(b)(4).

On 12 March 2026 an analyst reintegrates a chromatogram for batch HT-2611 and a QA reviewer approves the record. The expected trail (fictional values):

Time (UTC)	User / role	Action	Old value	New value	Reason
2026-03-12 09:14:05	jmeier / QC analyst	Result saved	none	97.8%	Initial processing
2026-03-12 11:02:41	jmeier / QC analyst	Reintegration	97.8%	98.6%	Baseline error, deviation DV-0412
2026-03-12 14:07:19	akeller / QA reviewer	E-signature	Unsigned	Approved	Second-person review, 211.194(a)(8)

The approved record displays "A. Keller, 2026-03-12 14:07 UTC, Approved (second-person review)": name, date and time, and meaning, as 11.50 requires.

A gap assessment found four issues:

1. **Overwritten results.** The CDS retained only the latest integration; 97.8% survived only in the trail. This conflicts with 11.10(e) ("shall not obscure") and with FDA's statement that each reprocessed result be retained (data integrity Q&A, Q14).
2. **Shared login.** A balance PC used a generic "QCLAB" account, so actions cannot be attributed to one person: 11.10(d), 11.10(g), 11.100(a), and data integrity Q&A Q5.
3. **Signature image.** Exported reports carried a scanned signature graphic, which can be copied by ordinary means (11.70).
4. **Undocumented time zone.** The server stored local time with no stated reference (2003 guidance, fn. 5).

If HT-2611 expires on 30 June 2028, 211.180(a) sets retention to at least 30 June 2029, and 11.10(e) keeps the audit trail at least as long. Contract-laboratory certificates arrive through a portal whose accounts the laboratory administers, which on a literal reading of the definition in 11.3(b)(9) makes it an open system for Halden (FDA has published no classification of vendor-hosted portals), so the assessment also looks for the 11.30 measures.

Gap-assessment checklist

1. Which predicate rule requires the record, and is reliance on electronic or paper documented?
2. Is the system closed or open under 11.3(b)(4) and (9)?
3. Does documented, risk-based validation cover detection of invalid or altered records (11.10(a))?
4. Can complete human-readable and electronic copies be produced, with audit trails (11.10(b))?
5. Does the audit trail record who, when, old and new value, independently, and is it protected from editing or disabling (11.10(e))?
6. Are prior values, including reprocessed results, retained?
7. Are all accounts individual, with authority checks (11.10(d), (g); 11.100(a))?
8. Do signed records show name, date and time, and meaning on screen and in print (11.50)?
9. Can a signature be copied to another record by ordinary means (11.70)?
10. Are two components, session rules and credential controls enforced (11.200, 11.300)?
11. Has the 11.100(c) certification been submitted?
12. Do retention periods for records and audit trails come from the predicate rule?

For sector context, see pharma. Whatever system holds a regulated record, the test a reader should be able to run is the one 11.10(e) describes: who changed this value, when, and what it said before.

Sources

1. 21 CFR Part 11 (eCFR, current to 27 October 2026): full text, source and amendment notes.
2. 21 CFR 11.1: scope, exclusions.
3. 21 CFR 11.3: definitions.
4. 21 CFR 11.10: closed-system controls, audit trail.

5. 21 CFR 11.30: open-system controls.
6. 21 CFR 11.50: signature manifestations.
7. 21 CFR 11.70: signature/record linking.
8. 21 CFR 11.100: uniqueness, identity, certification.
9. 21 CFR 11.200: signature components.
10. 21 CFR 11.300: ID code and password controls.
11. FDA, Part 11 Scope and Application, guidance page: status, docket.
12. FDA, Part 11 Scope and Application (PDF, August 2003): narrow scope, enforcement discretion, legacy systems.
13. FDA, Clinical Investigations Q&A, guidance page: status, October 2024.
14. FDA, Clinical Investigations Q&A (PDF, October 2024): audit trail content, signatures.
15. FDA, Data Integrity and Drug CGMP Q&A, guidance page: status, December 2018.
16. FDA, Data Integrity and Drug CGMP Q&A (PDF, December 2018): ALCOA, audit trail review, shared logins.
17. 21 CFR 211.68: computer controls under drug CGMP.
18. 21 CFR 211.180: batch record retention.
19. 21 CFR 211.194: laboratory records, second-person review.
20. 21 CFR 312.62: investigator record retention.
21. Change of Address; Technical Amendment, 88 FR 13018, 2 March 2023: nonsubstantive update to the 11.100(c) submission address.

Source links

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

1. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/subpart-A/section-11.1
2. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11
3. https://www.fda.gov/media/75414/download
4. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/subpart-A/section-11.3
5. https://www.fda.gov/media/166215/download
6. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/subpart-B/section-11.10
7. https://www.fda.gov/media/119267/download
8. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/subpart-B/section-11.30
9. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/subpart-B/section-11.50
10. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/subpart-B/section-11.70
11. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/subpart-C/section-11.100
12. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/subpart-C/section-11.200
13. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/subpart-C/section-11.300
14. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application
15. https://www.federalregister.gov/documents/2023/03/02/2023-04010/change-of-address-technical-amendment

16. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/electronic-systems-electronic-records-and-electronic-signatures-clinical-investigations-questions
17. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-integrity-and-compliance-drug-cgmp-questions-and-answers
18. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-C/part-211/subpart-D/section-211.68
19. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-C/part-211/subpart-J/section-211.180
20. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-C/part-211/subpart-J/section-211.194
21. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-D/part-312/subpart-D/section-312.62

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.