

The Handoff Is in Validation Scope

A companion reading from the clinical-systems vendor seat — why the integration boundary, not the device, is where the regulated record is made

Prepared for	EDC, eCOA and RTSM / IRT vendors, and the sponsors and CROs that integrate them.
Subject	Why the integration boundary between the device and a validated clinical system is where the regulated record is made, and what has to survive the handoff.
Status / Date	Final — 1 September 2026
Version	1.0
Prepared by	Rudiger Mees

Executive summary

The answer. Under FDA, the source data are located in the durable electronic data repository — the platform receiving the feed — and FDA does not intend to inspect individual digital health technologies for source-data verification. That puts your integration boundary, not the device, at the center of the evidence: it is where the regulated record is made. The EU position is not identical — the EMA guideline still expects device-side controls, so the record's integrity from capture to repository remains the sponsor's to evidence.

What that requires. The interface is in validation scope, not just the systems it connects.¹ Source, original capture time, attribution and audit context must be carried across it and provable afterwards — and where a change on either side alters the interface, it is a change event requiring revalidation.

What to do. Bring the interface inside the validation plan, map provenance field by field, test for silent metadata loss rather than assume it away, and hold the boundary evidence ready. In qointa's assessment the device-side and system-side audit records should also be reconciled at the seam — no instrument prescribes that method, and it is a recommendation, not a requirement.

¹ FDA, Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations: Questions and Answers (final, October 2024), Q23: for DHTs "electronic source data are considered to be located in the durable electronic data repository" and "FDA does not intend to inspect individual DHTs for source data verification". See also FDA, Digital Health Technologies for Remote Data Acquisition in Clinical Investigations (final, December 2023), s.IV.G.

The source record is the repository, not the device — which puts your handoff at the center of the evidence

The boundary is where the regulated record is made, so it is the boundary, not the device, that has to be validated and inspectable

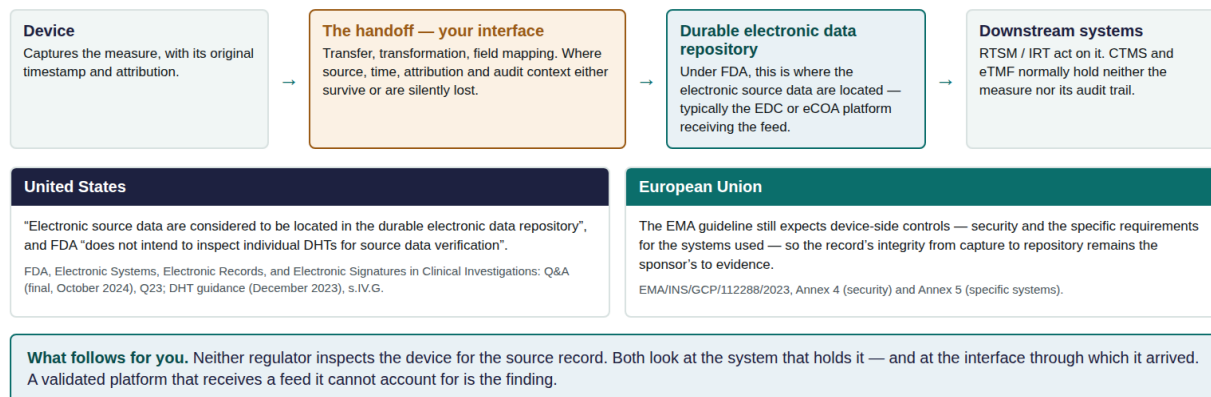


Figure 1 — The source record is the repository, not the device, which puts your handoff at the center of the evidence.

1. The boundary, not the device, is where the regulated record is made

This is a companion edition of qointa's position-paper series, read from the clinical-systems vendor's seat — principally EDC, eCOA and RTSM / IRT, the platforms that actually receive device data. The device — directly, or through the phone or gateway that relays for it — feeds your validated systems, and the integration boundary between them is itself in validation scope: provenance, timestamps and audit context must survive the transfer into your platform. This edition summarizes the position set out in QPP-20 — EHR Integration; the sources are cited there in full.

It is addressed to clinical-systems vendors and to the sponsors and CROs that integrate them. Four things have to survive the handoff, and each has an artifact that proves it did (Figure 2).

Regulatory basis

The positions in this edition rest on the following sources. Pin-cites are in the footnotes; the full argument is in the numbered papers.

- **FDA**, Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations: Q&A (final, October 2024), **Q23** — source data are located in the durable electronic data repository; FDA does not intend to inspect individual DHTs.
- **FDA**, Digital Health Technologies for Remote Data Acquisition in Clinical Investigations (final, December 2023), **s.IV.G**.
- **EMA/INS/GCP/112288/2023**, Annex 2 (validation, data transfer and interfaces), Annex 4 (security), Annex 5 (specific systems), Annex 6 (clinical systems).
- **21 CFR 11.10(a) and 11.10(e)** — validation of systems; secure, time-stamped audit trails.
- **ICH E6(R3)**, s.3.6 — the sponsor retains ultimate responsibility; a vendor's duties arise by contract.
- Reconciliation of the device-side and system-side audit records is **qointa's recommendation**; no instrument prescribes the method.

How this fits the full framework

This companion is keyed to Section 12 of the Regulatory Impact Assessment (QPP-00 — Regulatory Impact Assessment (RIA)). The numbered papers carry the detail — the ties most relevant to a clinical-systems vendor are:

- **QPP-10 — Data Integrity.** Establishes the provenance and audit trail that must survive the handoff.
- **QPP-14 — Interoperability.** The integration boundary is part of the validated system.
- **QPP-06 — Inspection-Readiness.** What an inspector asks for when the record arrived through an interface.
- **QPP-07 — Change Control.** Interface changes on either side are change events that can break provenance.
- **QPP-20 — EHR Integration.** The full treatment of the device-to-clinical-system boundary.

Four things must survive the handoff, and each one has an artefact that proves it did

"The interface is validated" is a claim; these four are the evidence behind it

What must survive	How it is lost	The artefact that proves it	Where the expectation comes from
The original capture time	Receipt time overwrites capture time in the mapping, and nothing records that it did.	A field-level map showing capture time carried, plus a negative test that proves it is not overwritten.	EMA/INS/GCP/112288/2023, Annex 2; FDA Part 11 Q&A (October 2024)
Attribution	The feed writes a service account, and who or what produced the measure is no longer recoverable.	Attribution fields mapped end to end, with the device-side identifier retained in the record.	21 CFR 11.10(e); ALCOA++ (attributable)
Audit context	The device-side audit trail stays on the device; the system-side trail starts at receipt.	Reconciliation evidence between the two records at the seam.	qointa's recommendation — no instrument prescribes the method
The interface itself	A change on either side is treated as minor and ships without revalidation.	The interface inside the validation scope, with change records and revalidation triggers.	EMA guideline, Annex 2; QPP-07 — Change Control

One boundary that is not yours. RTSM / IRT and eCOA integrations carry device data. CTMS and eTMF normally do not: they hold operational and document records, and pulling them into this analysis blurs the scope rather than widening it.

A validated system is only as reliable as the data crossing into it — and the four rows above are what turns that sentence into an evidence package.

Figure 2 — Four things must survive the handoff, and each one has an artifact that proves it did.

2. Four facts about the handoff that decide whether your platform is defensible

- **The interface is in scope.** The integration between the device and your system must be validated, not only the systems at either end.
- **Provenance must survive the handoff.** Source, time and attribution cannot be lost in transit.
- **Two audit records meet at the seam.** In qointa's assessment they should be reconcilable; no instrument prescribes the method.
- **You inherit upstream integrity.** A validated platform can still receive data it cannot account for — and the sponsor remains ultimately responsible for the trial data either way.

3. Four perimeters meet at the handoff, and each has an evidence artifact

Each perimeter is something the handoff pulls into scope. The third column names the **vendor action and the evidence** that discharges it — what you do, and what a sponsor auditor or GCP inspector would expect to see. The data-integrity row is flagged because provenance lost at the boundary cannot be recovered downstream (Figure 2).

Perimeter / topic	What it means for you	Vendor action / evidence	Series paper
Data integrity	Provenance, timestamps and audit trail across the handoff.	Map and validate the provenance fields; reconcile the two audit trails.	QPP-10
Interoperability	The integration boundary is part of the system.	Bring the interface into the validated system boundary.	QPP-14
Inspection	The handoff is examined as part of the evidence for the record, wherever it is held.	Hold boundary evidence — mapping, tests, reconciliation — ready for inspection.	QPP-06
Change control	Interface changes on either side are change events.	Treat interface changes as change events; revalidate.	QPP-07

4. Three ways provenance is lost without anyone noticing

- **Silent loss of metadata at the boundary.** Timestamps and audit context can drop in transfer.
- **Reconciliation gaps between audit trails.** Device-side and system-side records must align.
- **Interface changes treated as minor.** An integration change can break provenance.

5. Six artifacts bring the boundary into validation

Six artifacts turn “the interface is validated” from a claim into an evidence package. Each line is a thing that exists on file (Figure 2).

Checklist item	Evidence that it is done
The interface is inside the validation scope.	A validation plan covering the interface, not only the systems it connects.
Provenance fields mapped device-to-system.	Field-level mapping of source, timestamp and attribution.
Device-side and system-side audit records reconcile at the seam.	Reconciliation evidence between device- and system-side records.
Metadata loss tested for, not assumed.	Negative tests confirming no silent drop in transfer.
Interface changes run under change control.	Change records and revalidation triggers for the interface.
Boundary evidence ready for inspection.	A boundary evidence package covering the handoff — mapping, tests, change records.

Provenance mapping template (illustrative)

A per-field map that shows provenance survives the handoff into your system:

- **Field:** *[data element] — [device representation] → [system representation]*.
- **Source & timestamp:** *[original capture time carried, not overwritten by receipt time]*.
- **Attribution:** *[who / what produced it, preserved across the transfer]*.
- **Audit reconciliation:** *[how device- and system-side audit records align at the seam]*.

6. Evidence at the seam is what makes the whole record defensible

Four moves, in order of what breaks first

A validated clinical system is only as reliable as the data crossing into it. Evidencing the boundary — provenance, timing, reconciliation and change control — is what makes the record defensible from capture to repository, and it is the one part of that chain that no one upstream can supply for you.

- **Bring the boundary into validation scope** so the interface is validated, not just the endpoints it connects.
- **Map provenance field by field** so source, time and attribution survive the handoff rather than dropping silently.
- **Reconcile the two audit trails** so device-side and system-side records align at the seam.
- **Treat interface changes as change events** so an integration change never breaks provenance unnoticed.

Example evidence statement for sponsors

A short, defensible framing a clinical-systems vendor can provide so the sponsor can rely on the handoff:

“The integration boundary is within our validation scope. We map source, original capture time and attribution field by field so provenance survives the handoff, test for silent metadata loss rather than assume it away, reconcile our audit record with the device-side record at the seam, and treat any interface change as a change event requiring revalidation. The boundary evidence is held ready for inspection.”

Scope and status. This is a companion edition summarizing qointa's position-paper series from one stakeholder's perspective, keyed to Section 12 of the Regulatory Impact Assessment (QPP-00 — Regulatory Impact Assessment (RIA)). The sources for the positions taken here are cited in the footnotes and in the Regulatory basis box; the full treatment is in the numbered papers. It is not legal advice, and any specific position should be confirmed with qualified regulatory counsel.