

Integrity is decided at the point of capture on the device — attribution, time and protection against alteration are fixed there, and no validated database can restore them later.

"Our EDC is validated, so data integrity is handled" stops one system too late: the record was captured upstream. **Engineer and validate the ALCOA++ controls on the device — on-device audit trail, trusted time, attributed entry, signature binding and integrity across the sync seam — and feed the timing and offline-capture triggers into the Trigger Register.**

THE PICTURE Integrity is decided at capture, but FDA and the EMA guideline look for it in different places

FDA — source data sit in the repository

- Part 11 Q&A (Q23) and DHT guidance (s.IV.G): DHT electronic source data are located in the durable electronic data repository
- FDA does not intend to inspect individual DHTs for source data verification
- It asks instead for a validated, prompt transfer whose date and time enter the audit trail (Q22)
- System clock must be controlled (Q14)

vs

EMA guideline — controls on the device itself

- No user-modifiable date, time or time zone on the data-entry device where it is the timestamp (s.5.5)
- Locally held data must not change without the originator's knowledge before saving (s.6.2.1)
- ePRO devices and BYOD apps are within scope (Annex 5, A5.1)
- The sponsor must never hold exclusive control of the data (s.6.6)

The practical consequence is the same under both: whatever the device did before sync is what the repository faithfully preserves, flaws included. qointa's device-side design standard satisfies the stricter regime and is the only way to evidence the record in either.

QOINTA'S POSITION Four positions that move integrity from the database to the device

Capture fixes integrity

Once the device captures regulated data, the record's attribution, timestamp and protection against alteration are set there, before any upload — on two devices in sequence where a wearable hands off to a gateway.

Time is a control

A user-modifiable device clock used as the timestamp is an integrity weakness wherever timing matters; the achievable control is trusted server or network time plus discrepancy detection.

A validated database does not cover the device

The back-end can be flawless while the device-side record is not trustworthy. Integrity lost at capture cannot be reconstructed afterwards — the loss is irrecoverable.

Part 11, the EMA guideline and ICH E6(R3) all reach the point of capture

Part 11 §11.10(d)-(e), §§11.50 and 11.70; EMA s.4.5, 5.5, 6.2.1, 6.6 and Annex 5; ICH E6(R3) Section 4 and s.3.16. EU GMP Annex 11 is a manufacturing instrument, not the reference.

SIX QUESTIONS TO ANSWER ON THE DEVICE BEFORE ENROLLMENT

- 1 Build an on-device audit trail** of entries and changes before sync — without it, a change at capture is invisible (EMA s.6.2.1; Part 11 §11.10(e)).
- 2 Use trusted server or network time;** lock the device clock where it is the timestamp and detect and log discrepancies (EMA s.5.5; FDA Q14).
- 3 Attribute every entry** to the authenticated participant or user — an unattributable record cannot support the endpoint.
- 4 Bind each electronic signature** to the person and record, manifesting signer, date and time, and meaning (§§11.50, 11.70).
- 5 Protect the offline window and the sync seam** with a tamper-evident local store and integrity checks; validate across the BYOD fleet, not one reference device.
- 6 Retain the original record and metadata** through to decommissioning (QPP-13); CTR Art. 58 sets 25 years for the trial master file.

6

questions decide whether the device-side record is trustworthy

5

deployment facts that raise the device-side integrity weight and feed the RIA

8

device-side integrity checks to answer in the RIA

25 yrs

trial master file retention under CTR Art. 58

Read with care. The device-side controls are qointa's design standard: they satisfy the EMA guideline and exceed FDA's stated expectation. Scope is integrity at the point of capture only; back-end and infrastructure validation is a separate subject. The worked example is an illustrative composite.

READ NEXT

QPP-00 Regulatory Impact Assessment · QPP-05 Cybersecurity · QPP-06 Inspection-Readiness · QPP-07 Change Control · QPP-08 Trigger Register · QPP-13 Decommissioning

