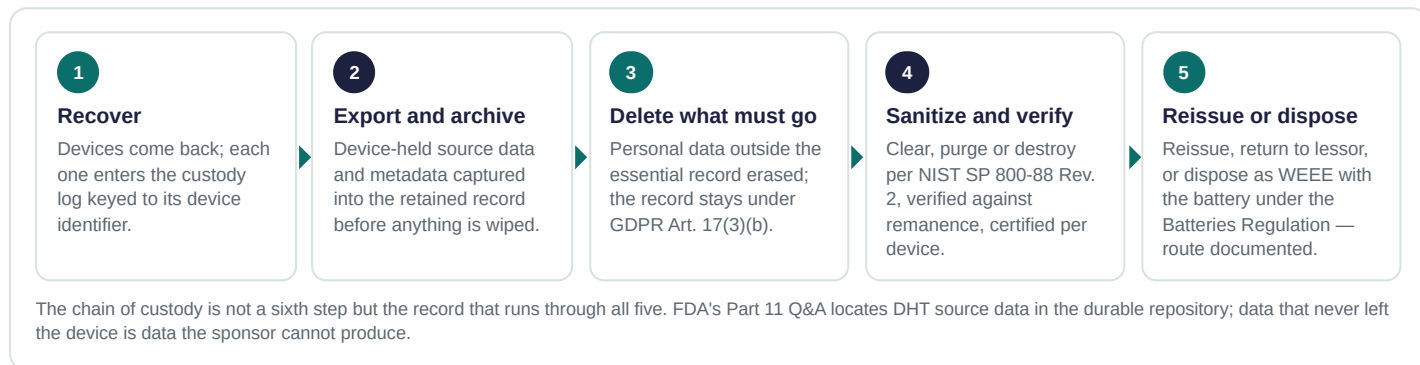


Export before you wipe, evidence every step per device, and decide in writing what is retained and what is erased — before the devices come back.

Data wiped before export cannot be recovered, and an unevidenced wipe cannot be shown — neither can be repaired after the fact. **Write the end-of-life plan into the RIA at the start: the five-step sequence, a custody log keyed to the device identifier, the retention schedule per jurisdiction and per-device vendor evidence.**

THE PICTURE

Export before wipe: five evidenced steps in a fixed order — reversed, the source data is gone and the erasure is unprovable



QOINTA'S POSITION Four duties that do not lapse with the last visit

The end of life is regulated too

Retention, deletion, wipe and disposal each carry obligations that do not end when the last visit does. "We'll just collect the devices" assumes none of them is binding.

Retain and delete are settled by legal obligation, not consent

The record is processed under a legal obligation (GDPR Art. 6(1)(c)), so erasure does not apply to it (Art. 17(3)(b)); consent withdrawal does not unwind collected data (CTR Art. 28(3)).

A wiped device still has a data-protection story

A factory reset that only removes file pointers does not address remanence. Erasure must be evidenced against the device identifier with a recognized method matched to the destination.

Chain of custody runs to the end

A recovered device carries identifiers and residual data until it is verifiably cleared; for an investigational device its return or disposal is itself a record the sponsor keeps.

FIVE ACTIONS THAT CLOSE THE LIFECYCLE CLEANLY

- 1 Sequence the end of life** — define export-before-wipe as the order and build it into the close-out plan.
- 2 Reconcile retain and delete** — document the legal basis for retention and the retention schedule, region by region, per data category.
- 3 Evidence the wipe** — use a recognized sanitization method, verify against remanence, certify per device and qualify the vendor.
- 4 Hold the chain of custody** — record each step against the device identifier, end to end; for BYOD, record participant confirmation.
- 5 Plan it early** — feed end-of-life triggers into the Trigger Register and put the plan in the RIA at the outset, not at close.

25 yrs

EU TMF retention after the end of the trial (CTR Art. 58)

10 / 15 yrs

EU device investigation retention, 15 for implantables (MDR Annex XV Chapter III s.3)

2 yrs

US sponsor retention after approval or completion (21 CFR 312.57(c) / 812.140(d))

9

end-of-life reconciliation questions to answer in the RIA before the devices come back

Read with care. Not legal advice; does not determine retention periods or deletion obligations for any specific study. Requirements are jurisdiction-specific and can conflict — confirm with regulatory and privacy counsel as of September 2026.

READ NEXT

QPP-00 Regulatory Impact Assessment · QPP-02 Data Residency and Cross-Border Transfer · QPP-08 Trigger Register · QPP-10 Data Integrity · QPP-12 Vendor Qualification and Oversight

