

A CRO and an investigator site are two different parties under GCP: the duties divide between them, and one control here belongs to neither.

Inspectors do not examine the device; they examine what the site did around it — consent versions, delegation and training, and whether device and app problems were escalated and recorded. **You cannot build an audit trail on a participant's own phone: that control belongs to the sponsor and the system vendor.**

THE PICTURE Five duties concentrate at the site, each with an owner — except one

Perimeter	What it means for you	CRO / site action / evidence
Data integrity	Using the study systems as designed; recording when they are not	Escalate device and app problems; never build a BYOD audit trail
Inspection	Producing the site-side record an inspection actually asks for	Keep consent versions, delegation, training and issue records current
Human factors / consent	Catching use problems; administering eConsent and re-consent	Log usability issues; control eConsent versions and re-consent process
Change control	Receiving and escalating app / OS change notifications	Route every change notice to the sponsor and the Trigger Register
Oversight	Performing vendor oversight as a delegated, overseen activity	Evidence the oversight you perform — it is itself overseen

The data-integrity row is flagged because it is the duty commonly assigned to sites that cannot perform it. Under FDA, source data sit in the durable repository; FDA does not intend to inspect individual DHTs.

QOINTA'S POSITION Four facts about your seat — and one control that is not yours

The CRO runs transferred work; the site is the investigator

Consent, delegation and the record of what happened are the site's; data management and monitoring are usually the CRO's.

Oversight you perform is itself overseen

Where the sponsor transfers vendor oversight to the CRO, ICH E6(R3) s.3.6.9 keeps it inside the sponsor's accountability — and expects evidence.

You see what participants encounter first

Usability problems, confusion and device failures reach you before anyone else — and only if you record them do they reach the sponsor at all.

The device-side audit trail is not yours to build

It is generated by the application and held in the repository; the sponsor and the system vendor own it, on BYOD as on provisioned devices.

FIVE RECORDS MAKE YOUR OPERATIONS DEFENSIBLE

- 1 Confirm who owns the device-side controls** — get the sponsor's written statement that audit trail, access and time are system-generated.
- 2 Control consent versions** — tie every consent and re-consent to the approved version in force; a superseded version is a serious deficiency.
- 3 Run a standing escalation routine** — a named path for app, device and OS change notices into the sponsor and the Trigger Register.
- 4 Evidence the oversight the CRO performs** — record the transferred vendor oversight, because it is itself overseen.
- 5 Keep the site-side record current** — consent versions, delegation and training, issue and deviation records, ready when asked for.

Read with care. The BYOD gap is reported from qointa's experience: it is discovered when someone asks the site for an audit trail it was never able to produce. Full argument and pin-cites are in QPP-10 and QPP-12.

READ NEXT

QPP-00 RIA (Section 12) · QPP-10 Data Integrity · QPP-12 Vendor Qualification and Oversight · QPP-06 Inspection-Readiness · QPP-07 · QPP-08 Trigger Register · QPP-09 · QPP-11



Summary of S10 1.0 — the full paper, with sources and figures, is published at qointa.com.

ICH E6(R3) s.2 (s.2.8), s.3.6 (ss.3.6.6–3.6.9) · FDA Electronic Systems Q&A (Oct 2024), Q23 · FDA DHT guidance (Dec 2023), s.IV.G · FDA Decentralized Elements (2024) · EMA/INS/GCP/112288/2023 · HMA/EC/EMA DCT paper v02

© qointa 2026 – Public – Uncontrolled when printed · Not legal advice; this summary does not classify any device.

qointa · DHT governance for clinical trials
sales@qointa.com · qointa.com