

# Where the Evidence Is Actually Made

A companion reading from the CRO and site seat — which duties are yours, which are the sponsor's, and which control belongs to neither of you

|               |                                                                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prepared for  | CRO leadership, project management, clinical operations, quality, data management and site staff.                                                          |
| Subject       | How the duties in a digital trial divide between the CRO as service provider and the investigator site — and which device-side controls belong to neither. |
| Status / Date | Final — 1 September 2026                                                                                                                                   |
| Version       | 1.0                                                                                                                                                        |
| Prepared by   | Rudiger Mees                                                                                                                                               |

## Executive summary

**The answer.** A CRO and an investigator site are two different parties under GCP, and the duties divide between them. The CRO is a service provider performing activities transferred by the sponsor — and where it performs oversight on the sponsor's behalf, that transferred activity is itself overseen. The investigator holds duties of their own: consent, delegation, qualified staff, and reporting what actually happened.<sup>1</sup>

**What inspection actually looks at.** Not the device. Under FDA, the electronic source data are located in the durable electronic data repository, and FDA does not intend to inspect individual digital health technologies for source-data verification. What is examined at your sites is the process around the device: consent versions, delegation and training, and whether device and app problems were escalated and recorded.

**What to do.** Control consent versions, keep the delegation and training record current, run a standing check for app and device problems with a named escalation path, and evidence any oversight you perform for the sponsor. What you cannot do is build an audit trail on a participant's own phone — that control belongs to the sponsor and the system vendor, and a site asked to own it should say so in writing.

<sup>1</sup> ICH E6(R3) Principles and Annex 1 (Step 4, 6 January 2025; EU effective 23 July 2025): section 2 sets out the investigator's duties, including s.2.8 (informed consent); s.3.6 sets out the sponsor's use and oversight of service providers, including ss.3.6.6–3.6.9 on assessing suitability, access to procedures and performance metrics, and oversight of transferred activities “including activities further subcontracted by the service provider”. Annex 2 reached Step 4 on 3 June 2026 and is effective in the EU from 15 January 2027.

## Inspectors do not examine the device — they examine what the site did around it

The source record sits in the repository; the site's evidence is the process that produced it, and that is what an inspection asks for

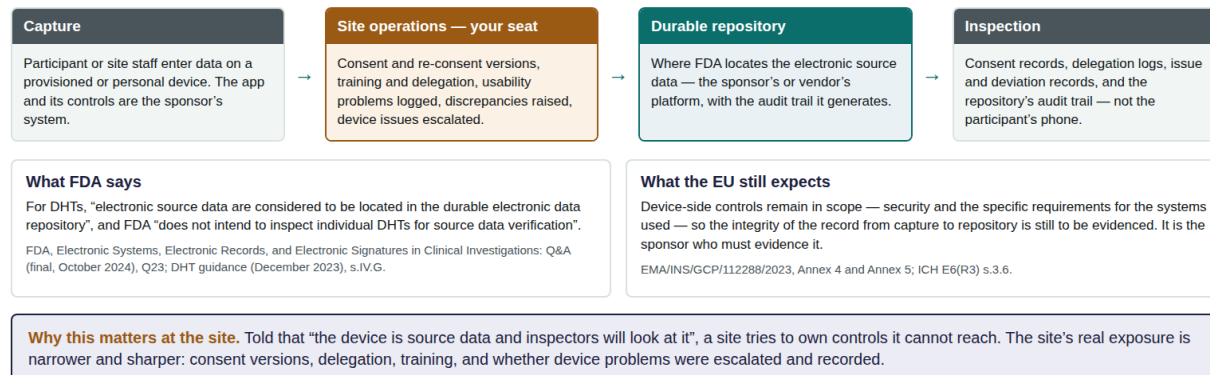


Figure 1 — Inspectors do not examine the device; they examine what the site did around it.

## 1. The CRO and the site are two parties, and the duties divide between them

This is a companion edition of qointa's position-paper series, read from the CRO and site seat. **You operate the trial at the point where participants and devices meet**, and — where the sponsor transfers oversight to the CRO — you perform an activity that is itself overseen. This edition summarizes the positions set out in QPP-10 — Data Integrity and QPP-12 — Vendor Qualification and Oversight; the sources are cited there in full.

It is addressed to CRO leadership, project management, clinical operations, quality and data management, and to investigator sites and their staff. Where a duty falls differently on the CRO and on the site, this edition says so (Figure 2).

### 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 CRO and its sites are:

- **QPP-10 — Data Integrity.** What the record has to show from capture to repository — and which party builds each part of it.
- **QPP-06 — Inspection-Readiness.** What an inspector asks a site for, and what it does not ask for.
- **QPP-09 — Human Factors** and **QPP-11 — eConsent.** Use problems surface where participants are; consent versions are the investigator's to control.
- **QPP-07 — Change Control.** App and OS changes are change events — usually detected by the vendor's telemetry, escalated through you.
- **QPP-12 — Vendor Qualification and Oversight.** When the CRO oversees vendors for the sponsor, that transferred activity is itself overseen.

### 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.

- **ICH E6(R3)**, section 2 (investigator duties, incl. s.2.8 informed consent) and s.3.6 (sponsor use and oversight of service providers, ss.3.6.6–3.6.9).
- **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**; Conducting Clinical Trials With Decentralized Elements (final, September 2024).
- **EMA/INS/GCP/112288/2023**, Annex 4 (security), Annex 5 (specific systems, incl. A5.3 eConsent).
- **HMA/EC/EMA** Recommendation paper on decentralized elements in clinical trials, Version 02 (1 October 2025).
- GCP inspections are performed by **FDA (BIMO)**, **EU national competent authorities** (EMA coordinates) and the **MHRA**.

## 2. Four facts about your seat — and one control that is not yours

- **The CRO operates transferred activities; the site holds the investigator's duties.** 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.** Usability problems, confusion and device failures reach you before they reach 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.

## 3. Five duties concentrate at the site, and each has a named owner

Several duties concentrate where participants and devices meet. Each maps to a paper — and to a concrete record on your side. The last row is flagged because it is the one commonly assigned to sites that cannot perform it (Figure 2).

| Perimeter / topic     | What it means for you                                                              | Paper | CRO / site action / evidence                                                                                                                   |
|-----------------------|------------------------------------------------------------------------------------|-------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data integrity</b> | Using the study systems as designed, and recording what happens when they are not. | 10    | Escalate device and app problems; confirm the sponsor's system carries the audit trail — do not attempt to build one on a participant's phone. |
| <b>Inspection</b>     | Producing the site-side record that an inspection actually asks for.               | 6     | Keep consent versions, delegation and training, and issue records complete and current.                                                        |

| Perimeter / topic              | What it means for you                                          | Paper | CRO / site action / evidence                                                                        |
|--------------------------------|----------------------------------------------------------------|-------|-----------------------------------------------------------------------------------------------------|
| <b>Human factors / consent</b> | Catching use problems; administering eConsent and re-consent.  | 9, 11 | Log usability issues; control eConsent versions and re-consent process.                             |
| <b>Change control</b>          | Receiving and escalating app / OS change notifications.        | 7     | Route every change notice to the sponsor and into the Trigger Register (QPP-08 — Trigger Register). |
| <b>Oversight</b>               | Performing vendor oversight as a delegated, overseen activity. | 12    | Evidence the oversight you perform — it is delegated, and itself overseen.                          |

## CRO and site are different parties under GCP — and one duty here belongs to neither

The CRO is a service provider performing transferred activities; the investigator holds duties of their own. Assigning a control to the wrong one is how it ends up unowned

| The duty                                                                         | CRO — service provider                                                               | Investigator site                                                           | Basis                                                                  |
|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------|
| <b>Consent and re-consent versions</b>                                           | Builds and monitors the process; checks version control at monitoring visits.        | Obtains consent and documents it, against the approved version in force.    | ICH E6(R3) s.2.8; EMA guideline Annex 5.3 (eConsent)                   |
| <b>Delegation, training and access</b>                                           | Maintains the training record where contracted to.                                   | Delegates tasks to qualified staff and keeps the log.                       | ICH E6(R3) section 2 (investigator)                                    |
| <b>Escalating device and app problems</b>                                        | Routes the escalation to the sponsor and into the Trigger Register.                  | Reports what staff and participants encounter, promptly and in writing.     | ICH E6(R3) s.3.6; QPP-08 — Trigger Register                            |
| <b>Oversight performed for the sponsor</b>                                       | Performs it — and evidences it, because the transferred activity is itself overseen. | Not a site duty.                                                            | ICH E6(R3) s.3.6.6–3.6.9                                               |
| <b>Audit trail, access control and trusted time on a participant's own phone</b> | Cannot build it. Can check that it exists and is evidenced.                          | Cannot build it. Has no administrative control over a participant's device. | Sponsor and system vendor — EMA guideline Annexes 4 and 5; FDA Part 11 |

**The misallocation to avoid.** Telling sites to “maintain the audit trail on BYOD devices” assigns a control to the one party that cannot perform it. The audit trail is generated by the application and held in the repository; what the site can do is use the app as designed, and escalate when it does not behave.

A control assigned to a party that cannot perform it is not a control. It is a finding waiting for an inspection.

Figure 2 — CRO and site are different parties under GCP, and one duty here belongs to neither.

## 4. Three things that go wrong where participants and devices meet

- **BYOD treated as a site responsibility.** A participant's own phone cannot be administered by the site; in qointa's experience the gap is discovered when someone asks the site for an audit trail it was never able to produce.
- **Informal re-consent across sites.** Consent obtained against a superseded version is a serious deficiency — the investigator's duty under ICH E6(R3) s.2.8, and one an inspection will test directly.
- **A change notice that stops at the site.** If a vendor's notification is not routed onward, no one assesses the change until it shows up in the data.

## 5. Five records make your operations defensible

Five records do the work. Each is a thing that exists on file, and each sits with the party that can actually produce it (Figure 1).

- **Confirm who owns the device-side controls** — get the sponsor's written statement that the audit trail, access control and trusted time are generated by the study system, on BYOD as on provisioned devices.
- **Control consent versions** — every consent and re-consent tied to the approved version in force and a documented process (QPP-11 — eConsent).
- **Run a standing escalation routine** — a named path for app, device and OS change notices, into the sponsor and the Trigger Register (QPP-07 — Change Control; QPP-08 — Trigger Register).
- **Evidence the oversight the CRO performs** — record the transferred vendor oversight, because it is itself overseen (QPP-12 — Vendor Qualification and Oversight).
- **Keep the site-side record current** — consent versions, delegation and training, issue and deviation records, ready when they are asked for (QPP-06 — Inspection-Readiness).

## 6. Owning the right duties is what makes you a lower-risk partner

A CRO and its sites are where the trial meets the participant, and that is where the record of how the data came to exist is made. **Owning the duties you can actually discharge — and saying plainly which ones you cannot — is what makes you the partner a sponsor can defend.**

### How qointa can help

qointa maps device-side controls to the party that can perform them, reviews consent-version and escalation processes across a site network, and prepares the site-side evidence a GCP inspection asks for. [info@qointa.com](mailto:info@qointa.com)

### 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.