

On BYOD the participant and their own phone become part of the instrument — and every obligation that follows anchors to the person, not to trial hardware.

The study team, not the participant, discharges those obligations: usability on the handset they hold, eConsent bound to the right person, lawful processing of special-category health data, and attribution of every entry. **Beneath all four: a sponsor-provided device must be available, so no one is excluded for lacking a phone.**

THE PICTURE Four obligations anchor to the participant; the team discharges all

Perimeter	What it means for the participant	Study-team action and evidence
Human factors	Usability for their real device and capability	Test across the real device and OS range; offer a sponsor device
Consent	Valid, informed eConsent bound to the participant	Evidence eConsent bound to the right person, incl. remote identity
Data protection	Lawful basis, transparency and rights over special-category data	Record lawful basis and Art. 9 condition; erasure within Art. 17(3)
Data integrity	Attribution of entries to the right participant	Evidence attribution, including for assisted or proxy entry

The consent row is flagged because identity is where remote, electronic consent most often fails. Illustrative composite — not a specific study.

QOINTA'S POSITION Four obligations anchor to the participant; none can be delegated to them

Their device is part of the instrument

On BYOD the participant's hardware and settings shape the data; the handset you did not choose sets the floor for data quality, and the interface you validated is not the one everyone sees.

Their behavior shapes data quality

Use-error and non-adherence become missing or wrong data — and when a carer enters data, the audit trail must show who acted, which the standard self-entry model does not.

Their data and rights anchor here

Lawful basis, transparency and data-subject rights attach to the person — but erasure only within the limits trial law sets (GDPR Art. 17(3); CTR Art. 28(3)).

Their consent must be valid, informed and bound to them

Identity is the weak point when consent is electronic and remote; the signer must be confirmed as the participant or their legally authorised representative.

SIX ACTIONS KEEP BYOD DATA USABLE AND ATTRIBUTABLE

- 1 Test usability on real devices** so the interface each participant actually sees is the one you validated against.
- 2 Bind eConsent to the right person** so remote, electronic consent is valid and informed, not merely acknowledged.
- 3 Handle data rights accurately** — record the lawful basis and Art. 9 condition, meet transparency duties, answer erasure within Art. 17(3).
- 4 Resolve attribution up front** so assisted or proxy entry never leaves data attributed to the wrong person.
- 5 Plan data clearance from the personal device** at close-out — a storage-limitation question distinct from the erasure right.
- 6 Offer a sponsor-provided device** so owning a suitable handset is never a condition of taking part; record who BYOD would exclude.

Read with care. Clearing trial data from a handset the trial never owned as part of close-out rests on qointa's assessment of storage limitation under GDPR Art. 5(1)(e). Figures are illustrative composites, not a specific study.

READ NEXT

QPP-09 Human Factors · QPP-10 Data Integrity · QPP-11 eConsent · QPP-13 Decommissioning · QPP-17 Representativeness · QPP-02 Data Residency · QPP-22 Continuous Monitoring



Summary of S11 1.0 — the full paper, with sources and figures, is published at qointa.com.

FDA DHT guidance (Dec 2023), s.III · HMA/EC/EMA DCT paper v02 · EMA/INS/GCP/112288/2023, Annex 4, A5.1, A5.3 · ICH E6(R3) 2.8 · FDA/OHRP eConsent Q&A (2016) · GDPR Arts 5(1)(e), 9, 13–14, 17(3) · CTR Art. 28(3)

© 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