

eConsent is not a paper form on a screen: one signature engages three regulatory perimeters at once, and a gap in any one can invalidate the consent and the participant's data.

Signature binding, remote identity and comprehension, and country-by-country acceptance must be designed in before go-live, not assumed from a tablet and a tick-box. **Run the three-perimeter assessment in the RIA, map signature acceptance per country and per signer, bind every signature to a document version, and set the data-processing basis separately from the research consent.**

THE PICTURE One eConsent signature sits inside three perimeters at once, and each has its own rulebook

Perimeter	What it requires	Common pitfall
Electronic signature	Bound to the right person and version, with audit trail; Part 11 in the US, the eIDAS tier national law requires in the EU	A "mark" that does not manifest signer, time and meaning, or is not version-bound
Data protection and privacy	A lawful basis, transparency, and a distinction between research consent and the processing basis	Treating research consent as the data-processing basis — they are not the same
GCP / ethics	Ethics-approved content and process, version control, documented comprehension and re-consent	Informal re-consent after an amendment, with no record of who saw which version

Invalid consent is not a paperwork problem: consent obtained on the wrong version, or without valid signature or identity, is not the consent the ethics committee approved, and whether the data can be used becomes a question for the committee and the competent authority.

QOINTA'S POSITION Four positions that separate a valid eConsent from a form on a tablet

The signature must bind the right person to the right version

Under 21 CFR Part 11 a signature manifests signer, date and time, and meaning, linked to the record (§§11.50, 11.70). Process audit trail, version control, re-consent and withdrawal all attach to it.

Acceptance varies by jurisdiction — the CTR is silent

Art. 29(1) requires consent "written, dated and signed" and says nothing about electronic form. Belgium requires an advanced or qualified eIDAS signature, the Czech Republic a qualified one, Greece's ethics committee wet ink.

Remote consent must design in identity and comprehension

Without a person in the room, identity cannot be assumed from physical presence and comprehension loses face-to-face cues — knowledge checks and the impartial witness (ICH E6(R3) s.2.8.9; CTR Art. 29(1)) fill the gap.

Research consent is not the data-processing basis

The two are distinct and both must be addressed; identity and biometric verification data carry their own obligations (GDPR Art. 9(1); Art. 35 where large-scale).

SIX CONTROLS, ONE PER TRIGGER THAT RAISES THE ECONSENT WEIGHT

- 1 Deliver a Part 11 signature** manifesting signer, time and meaning, bound to the document version — the eIDAS tier national law requires in the EU.
- 2 Design identity and comprehension into the remote path:** ID verification, a knowledge check and, where needed, a remote witness; record the process.
- 3 Make re-consent a controlled workflow** on every amendment, with version-bound signatures and an audit trail of who saw which version.
- 4 Map acceptance per country and per signer** before go-live; provide a wet-ink path and the required signature tier where a jurisdiction demands it.
- 5 Build assent and representative-consent flows** where minors or legally designated representatives are enrolled (CTR Arts 31–32; 21 CFR 50 Subpart D).
- 6 Set the lawful basis and transparency for identity data** separately from the research consent; minimise and protect it (QPP-02).

3

perimeters engaged by one eConsent signature: e-signature, data protection, GCP / ethics

3

eIDAS signature tiers — simple, advanced, qualified; only qualified equals handwriting (Art. 25(2))

6

deployment facts that raise the eConsent weight and feed the RIA

8

remote eConsent checks to answer in the RIA before enrollment

Read with care. Acceptance of electronic signatures is jurisdiction- and ethics-committee-specific and must be confirmed with counsel and the responsible committee. China's NMPA position is qointa's understanding only, to be confirmed against the primary text. Worked example is an illustrative composite.

READ NEXT

QPP-00 Regulatory Impact Assessment · QPP-02 Data Residency and Cross-Border Transfer · QPP-06 Inspection-Readiness · QPP-08 Trigger Register · QPP-10 Data Integrity



Summary of QPP-11 1.0 — the full paper, with sources and figures, is published at qointa.com.

21 CFR Part 11 and 21 CFR 50.27 · FDA/OHRP eConsent Q&A (Dec 2016) · FDA Part 11 Q&A (Oct 2024) · EU CTR Arts 28(3), 29(1), 31–32 · eIDAS 910/2014 as amended by 2024/1183 · HMA/EC/EMA Recommendation paper V02 (1 Oct 2025) · EMA/INS/GCP/112288/2023 Annex 5 · ICH E6(R3) s.2.8 · HRA/MHRA statement (2018) · GDPR Art. 9(1)

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