

A networked trial device holding clinical data is a security artifact, and its security is a **data-integrity obligation** the sponsor must evidence.

If the device or its data can be tampered with, the GCP record built on it is no longer trustworthy — a breach is a data-integrity finding before it is anything else. **Map surfaces, controls and owners in the RIA before deployment, treat every patch and end-of-support event as a regulated change, and wire incident response to the reporting clocks.**

THE PICTURE

Every layer of the trial device carries a security obligation; an endpoint passcode covers only the first

Layer	Exposure	Key control
Device / OS	Lost, stolen, jailbroken or unpatched handsets, wearables, gateways	Encryption at rest, screen lock, remote wipe, enforced patch baseline
Application	Insecure storage, weak authentication, third-party SDKs	Secure SDLC (IEC 81001-5-1:2021), SBOM, vetted SDKs, strong authentication
Connectivity (eSIM / data plan)	Interception, rogue networks, remote-provisioning abuse	Transport encryption, trusted provisioning, traffic monitoring
Device management (MDM)	Fleet-wide configure-and-wipe platform — a high-value target	Hardened console, least privilege, MFA, audit logging (ISO/IEC 27001:2022)
Back-end / integrations	APIs and boundaries into EDC — integrity lost in transit	Authenticated APIs, integrity checks, network segmentation

"The phone has a passcode and the cloud is secure" covers one layer of five. A control owned by no one is a gap.

QOINTA'S POSITION Four positions: security is a data-integrity requirement owned across the whole chain

Security is a regulatory requirement, not hygiene

MDR Annex I (ss.17.1–17.4) and FD&C Act s.524B write it into the device; the Cyber Resilience Act and RED into the non-device handset, wearable or gateway; the EMA guideline into the trial record.

Security and data integrity are the same problem seen twice

ALCOA++ attributability, traceability and protection against alteration all depend on a tamper-resistant device. A weakness is a reason to doubt the GCP record — the sponsor's accountability.

Every update is a regulated change

"Never patch" leaves known vulnerabilities open; "patch freely" disturbs the validated state. Route every update through change control; end-of-support is itself a security trigger.

A breach starts several clocks at once

GDPR Art. 33 notification within 72 hours; CTR serious-breach reporting within 7 days (Art. 52); MDR vigilance (Arts 87–90) where a device is involved; Cyber Resilience Act reporting for a non-device product.

QUESTIONS TO ANSWER IN THE RIA BEFORE DEPLOYMENT

- Record the device as in-scope clinical infrastructure** — medical device, cyber device, or non-device product under the Cyber Resilience Act.
- Encrypt on-device clinical data at rest**, with screen lock and remote wipe enforced, and minimize local retention.
- Evidence a secure development lifecycle**, an SBOM and a vulnerability-management plan for the app; inventory and vet third-party SDKs.
- Harden the MDM console** — least privilege, MFA, audit logging — and qualify the vendor under QPP-12.
- Route every software and OS update through change control** (QPP-07), with revalidation of affected functions.
- Plan end-of-support refresh and incident response** mapped to the GDPR, CTR, vigilance and Cyber Resilience Act reporting clocks.

1 of 5

layers covered by "the phone has a passcode and the cloud is secure"

72 h

GDPR Art. 33 notification to the supervisory authority after a confirmed compromise

7 days

serious-breach reporting under the Clinical Trials Regulation (Art. 52)

11 Dec 2027

Cyber Resilience Act security-by-design and vulnerability-handling obligations apply

Read with care. The stakeholder allocation of controls is qointa's recommended assignment, not a statutory one. Cybersecurity requirements are jurisdiction-specific and evolving; frameworks are those most often engaged as of September 2026. Not legal advice.

READ NEXT

QPP-00 Regulatory Impact Assessment · QPP-07 Change Control · QPP-08 Trigger Register · QPP-10 Data Integrity · QPP-12 Vendor Qualification and Oversight

Summary of QPP-05 1.0 — the full paper, with sources and figures, is published at qointa.com.

EU MDR Annex I ss.17.1–17.4 · MDCG 2019-16 Rev. 1 · FD&C Act s.524B · FDA Cybersecurity in Medical Devices (Feb 2026) · Cyber Resilience Act (EU) 2024/2847 · RED Delegated Regulation (EU) 2022/30 · NIS2 (EU) 2022/2555 · EMA/INS/GCP/112288/2023 · ICH E6(R3) · 21 CFR Part 11 · IEC 81001-5-1:2021 · ISO/IEC 27001:2022 · ISO 14971:2019 · IEC 62304

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