

The console is **inside the trust boundary**: the sponsor cannot rely on the locked-down state without evidence from it — yet locking a device down does not make you a manufacturer.

MDR Art. 16(1)(b)–(c) presupposes a device and follows the party that specifies the configuration and its purpose — usually the sponsor, acting on your platform. **Harden and evidence console access, document the lock-down profile, run every push as a logged change event, and record per study whether Art. 16 is engaged.**

THE PICTURE Four perimeters land on the console, and each has an evidence artifact

Perimeter	What it means for you	Vendor action / evidence
Security (QPP-05)	The control plane is part of the attack surface; its compromise is the fleet's compromise.	Harden console access; evidence MFA, least-privilege and audit logging.
Configuration (QPP-00)	Lock-down must be documented against the study's intended use.	Record the lock-down profile against the intended use stated by the sponsor.
Economic operator (QPP-03)	Whether Art. 16(1)(b)–(c) is engaged, and by whom, turns on intended purpose.	Record, per study, whether the configuration engages Art. 16 for the sponsor or for you.
Change control (QPP-07)	Policy and OS pushes are change events across the fleet.	Notify, schedule and log pushes as change events — and say which are reversible.

A policy push is a fleet-wide change event, and most of it cannot be undone: a profile usually is reversible, an OS version usually is not.

QOINTA'S POSITION Four facts about the control plane a sponsor will ask you to evidence

Your console is a trusted system

Compromise of the control plane is compromise of the fleet; the fleet is only as secure as its management plane. Shared or weak console credentials are the first failure mode.

Lock-down is a configuration act, and it must be documented

Whether it changes the device's regulatory position depends on intended purpose, not on the push. Neither MDCG 2019-11 Rev. 1 nor MDCG 2023-4 treats a managed handset as a controlled platform.

Operator duties follow the intended purpose

MDR Art. 16(1)(b)–(c) attaches to the party that supplies the device under its own name or changes its purpose — normally the sponsor, not the vendor that applies the configuration.

Your changes ripple to every device

An unmanaged mid-study push can alter the state the sponsor validated, and the audit trail is the only record it happened. "We just manage devices" is itself a trusted, in-scope function.

FIVE MOVES, IN ORDER OF WHAT BREAKS FIRST

- 1 Harden and evidence console access** — MFA, named accounts, least privilege, session logging, no shared or default credentials.
- 2 Document the lock-down profile** so the configuration act is recorded against the intended use, not assumed.
- 3 Run every push under change control**: a notified, logged event, not a silent alteration of the validated state.
- 4 Assess operator duties up front** so constraining a device to medical use does not draw an unowned obligation for you or the sponsor.
- 5 Retain the audit trail of console actions** — who changed what, when — and make it available to the sponsor.

Read with care. That the Art. 16 question follows the party that specifies the configuration — usually the sponsor — is qointa's assessment. The edition is not legal advice; positions should be confirmed with qualified regulatory counsel.

READ NEXT

QPP-00 Regulatory Impact Assessment (Section 12) · QPP-03 Economic-Operator Roles · QPP-05 Cybersecurity · QPP-07 Change Control · QPP-12 Vendor Qualification and Oversight



Summary of S07 1.0 — the full paper, with sources and figures, is published at qointa.com.

MDR Art. 16(1)(b)–(c) · ICH E6(R3) s.3.6 · EMA/INS/GCP/112288/2023 Annexes 2, 3 and 4 · 21 CFR 11.10(d) and 11.10(e) · ISO/IEC 27001:2022 · MDCG 2019-11 Rev. 1 (June 2025) · MDCG 2023-4 (October 2023)

© 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