

The Control Plane Is Part of the Trust

A companion reading from the device-management vendor seat — what the control plane must evidence, and when constraining a device is someone else’s regulatory problem

Prepared for	Mobile-device-management and fleet-management vendors, and the sponsors that deploy them.
Subject	What a device-management platform must evidence for a trial, and when constraining a device engages MDR manufacturer obligations — and for whom.
Status / Date	Final — 1 September 2026
Version	1.0
Prepared by	Rudiger Mees

Executive summary

The answer. The console is inside the trust boundary, and the sponsor cannot rely on the locked-down state without evidence from it. Constraining a handset or gateway to medical use, on the other hand, does not by itself make you a manufacturer: the manufacturer obligations in MDR Art. 16(1)(b)–(c) presuppose a device and turn on who puts it on the market under their own name or changes its intended purpose. In qointa’s assessment that question follows the party that specifies the configuration and its purpose — usually the sponsor, acting on your platform.

Which rules. Four duties land on the control plane. Sponsor oversight of service providers under ICH E6(R3) s.3.6;¹ user management, security and change control of computerized systems under the EMA computerized-systems guideline;² access control and audit trail for electronic records under 21 CFR Part 11;³ and information-security management to a recognized standard.⁴

What to do. Harden and evidence console access, document the lock-down profile against the study’s intended use, run every push as a notified and logged change event, and record — per study — whether the configuration you are asked to apply engages Art. 16 for the sponsor or for you. That record is what turns a management contract into a function the sponsor can rely on at inspection.

¹ Regulation (EU) 2017/745 (MDR), Art. 16(1)(b) (making a device available on the market under one’s own name) and Art. 16(1)(c) (changing the intended purpose of a device already placed on the market) — both presuppose a device. In qointa’s assessment the party that specifies the constrained configuration and its purpose, normally the sponsor, is the one those obligations follow; the phrase “controlled platform” does not appear in MDCG 2019-11 Rev. 1 (June 2025) or MDCG 2023-4 (October 2023) and is not used here.

² ICH E6(R3) Principles and Annex 1 (Step 4, 6 January 2025; EU effective 23 July 2025), s.3.6 — sponsor oversight of service providers, including activities further subcontracted. Annex 2 reached Step 4 on 3 June 2026 and is effective in the EU from 15 January 2027.

³ EMA, Guideline on computerised systems and electronic data in clinical trials, EMA/INS/GCP/112288/2023 (GCP IWG, 7 March 2023): Annex 3 (user management), Annex 4 (security), Annex 2 (validation and change control).

⁴ 21 CFR 11.10(d) (limiting system access to authorised individuals) and 11.10(e) (secure, computer-generated, time-stamped audit trails recording operator entries and actions that create, modify or delete electronic records). Verified at <https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/subpart-B/section-11.10> on 1 September 2026.

Locking a device down does not, by itself, make you a manufacturer

The operator question turns on intended purpose, and on who decides it — not on who pushes the profile

The configuration act

You constrain a handset to the study app, disable stores and sideloading, and enforce the locked-down state across the fleet.

1. Is there a device at all?

The manufacturer obligations in Art. 16 presuppose a device. A general-purpose handset running an eCOA app is often not one.

MDR Art. 16(1); QPP-00 — RIA

2. Has the intended purpose changed?

Art. 16(1)(b): making a device available under your own name. Art. 16(1)(c): changing the intended purpose of a device already on the market.

MDR Art. 16(1)(b)–(c)

3. Who decided it?

The party that specifies the constrained configuration and its purpose is the one the obligation follows — usually the sponsor, on your platform.

qointa's assessment; QPP-03

Executing the sponsor's profile

You configure what the sponsor has specified. The intended purpose is the sponsor's; the operator question sits with them. Your duty is to document the profile against that purpose and hand over the evidence.

Specifying it yourself

You define, market or supply the constrained configuration as a medical use of your own. Then Art. 16(1)(b)–(c) is live for you and must be assessed before deployment, not after.

qointa's position. No MDCG guidance treats a managed handset as a "controlled platform", and none says lock-down removes a device from "general purpose". The safe practice is to record, per study, which of the two columns applies and why — an unrecorded answer is the finding.

Figure 1 — Locking a device down does not, by itself, make you a manufacturer: the operator question turns on intended purpose and on who decides it.

1. The platform that enforces the locked-down state is part of what the trial has to trust

This is a companion edition of qointa's position-paper series, read from the device-management vendor's seat. The platform that enforces a locked-down state is itself part of what the trial has to trust — and the configuration you apply may engage obligations that belong to whoever specified it. This edition summarizes the positions set out in QPP-03 — Economic-Operator Roles and QPP-07 — Change Control; the sources are cited there in full.

It is addressed to MDM and fleet-management vendors and the sponsors that deploy them. The series' **"one device, several perimeters"** view locates you: your control plane sits closest to the device, and the security, configuration and change perimeters are drawn around what it does (Figure 2).

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.

- **MDR Art. 16(1)(b)–(c)** — manufacturer obligations where a party supplies a device under its own name or changes its intended purpose.
- **ICH E6(R3)**, s.3.6 — sponsor oversight of service providers, including subcontracted activities.
- **EMA/INS/GCP/112288/2023**, Annexes 2, 3 and 4 — validation and change control, user management, security.
- **21 CFR 11.10(d) and 11.10(e)** — limiting system access; secure, time-stamped audit trails.
- **ISO/IEC 27001:2022** — information security management.
- **MDCG 2019-11 Rev. 1 (June 2025)** and **MDCG 2023-4 (October 2023)** — qualification of software and of software-plus-hardware combinations. Neither treats a managed handset as a "controlled platform".

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 device-management vendor are:

- **QPP-00 — Regulatory Impact Assessment (RIA).** The lock-down profile and the intended use it is documented against are recorded here.
- **QPP-03 — Economic-Operator Roles.** Who carries MDR Art. 16 obligations when a device is supplied or reconfigured for a study.
- **QPP-05 — Cybersecurity.** The control plane is part of the attack surface; its compromise is the fleet's compromise.
- **QPP-07 — Change Control.** Policy and OS pushes are change events that can alter the state the sponsor validated.
- **QPP-12 — Vendor Qualification and Oversight.** The sponsor's duty to qualify and oversee you, and what it will ask for.

A policy push is a fleet-wide change event — and most of it cannot be undone

The console is the one place where a single action reaches every device in the study at once

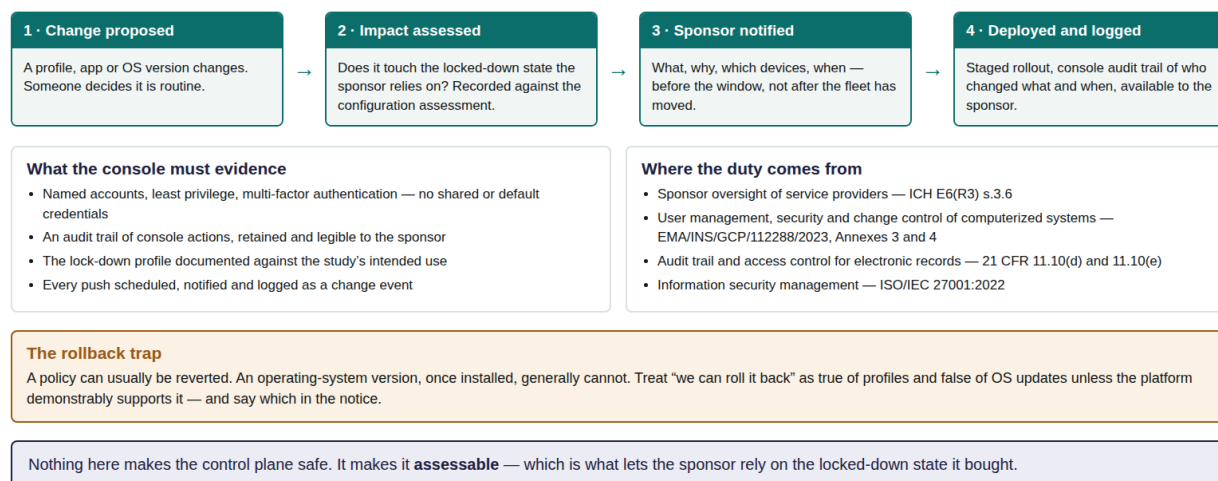


Figure 2 — A policy push is a fleet-wide change event, and most of it cannot be undone.

2. 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.
- **Lock-down is a configuration act, and it must be documented.** Whether it changes the device's regulatory position depends on the intended purpose, not on the push.
- **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.
- **Your changes ripple to every device.** A policy push is a change event across the fleet.

3. Four perimeters land on the console, and each has an evidence artifact

Each perimeter is something your platform pulls into scope. The third column names the **vendor action and the evidence** that discharges it — what you do, and what a sponsor auditor or GCP inspector would expect

to see. The security row is flagged because the control plane is the single point whose compromise reaches the whole fleet (Figure 2).

Perimeter / topic	What it means for you	Vendor action / evidence	Series paper
Security	The control plane is part of the attack surface to be secured.	Harden console access; evidence MFA, least-privilege and audit logging.	QPP-05
Configuration	Lock-down must be documented against the study's intended use.	Record the lock-down profile against the intended use stated by the sponsor.	QPP-00
Economic operator	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.	QPP-03
Change control	Policy and OS pushes are change events.	Notify, schedule and log policy and OS pushes as change events — and say which are reversible.	QPP-07

4. Three failure modes: shared credentials, unmanaged pushes and “we just manage devices”

- **Shared or weak console credentials.** The fleet is only as secure as its management plane.
- **Unmanaged policy pushes mid-study.** A configuration change can alter the state the sponsor validated, and the audit trail is the only record that it happened.
- **Assuming “we just manage devices.”** Management is itself a trusted, in-scope function.

5. Six artifacts make the control plane assessable

Six artifacts turn “we just manage devices” into a function the sponsor can rely on. Each line is a thing that exists on file, not a statement of intent (Figure 2).

Checklist item	Evidence that it is done
Console access is hardened.	MFA, named accounts, least-privilege and session logging.
No shared or default credentials.	Per-admin accounts; credential rotation policy on file.
Lock-down profile documented against intended use.	Profile spec mapped to the configuration assessment.
Operator-duty assessment recorded.	A per-study determination of whether Art. 16(1)(b)–(c) is engaged, and by whom.
Policy / OS pushes run under change control.	Scheduled, notified and logged change events.
Audit trail of console actions retained.	Who changed what, when — available to the sponsor.

Policy-push notification template (illustrative)

A lightweight notice that turns a fleet-wide push into a controlled change event the sponsor can rely on:

- **What & why:** *[policy / OS change] applied to [fleet / cohort] for [reason].*
- **Scope & timing:** *[devices affected] · [scheduled window] · [rollout / staged].*
- **Validated-state impact:** *[effect on the locked-down state, if any] and the assessment reference.*
- **Approval & rollback:** *[sponsor approval] · [whether the change is reversible — a profile usually is, an OS version usually is not] · [change-log entry].*

6. Evidence, not assurance, is what the sponsor is buying

Four moves, in order of what breaks first

The device-management platform is not neutral infrastructure: it is inside the trust boundary and, depending on who specifies the configuration, sometimes inside the operator chain. What the sponsor is buying is not an assurance that the fleet is locked down — it is the evidence that it is, and the record of every time that state changed.

- **Harden and evidence console access** so compromise of the control plane is not compromise of the fleet.
- **Document the lock-down profile** so the configuration act is recorded against the intended use, not assumed.
- **Run every push under change control** so a policy or OS change is a notified, logged event — not a silent alteration of the validated state.
- **Assess operator duties up front** so constraining a device to medical use does not draw an unowned obligation.

Example evidence statement for sponsors

A short, defensible framing an MDM vendor can provide so the sponsor can rely on the control plane:

“Console access is hardened with MFA, named accounts and least privilege, with full audit logging. The lock-down profile is documented against the intended use the sponsor has stated, and every policy or OS push is scheduled, notified and logged under change control — with the notice saying whether the change can be reversed. We have recorded, for this study, whether the constrained configuration engages MDR Art. 16(1)(b)–(c), and for whom.”

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.