

The eCOA / ePRO Vendor's Hidden Obligations

A companion reading from the vendor's seat — where your build and release choices place you inside the perimeters

Prepared for	eCOA / ePRO and DHT vendor leadership, product, quality and regulatory functions.
Subject	Where an eCOA / ePRO vendor sits across the regulatory perimeters of a digital trial.
Status / Date	Final — 1 September 2026
Version	1.0
Prepared by	Rudiger Mees

Executive summary

Settle two questions before a sponsor asks: is the app a medical device, and can you hand over the evidence package? "We're just the software provider" rarely describes where an eCOA / ePRO vendor lands. In the EU, software qualifies as medical device software (MDSW) where it acts on data beyond storage, communication or simple search **and** that action is for the benefit of an individual patient — scoring a questionnaire to generate trial data is not automatically either; alerting a clinician about a participant is a different matter.¹

Whatever the answer, you own evidence the sponsor cannot produce for you. Validation across every device type and operating system used in the trial, the audit trail and its time source, use-safety in the real population and a change log for every release are yours, because only you hold them.² Each release is a change event in a live trial, and the sponsor — which retains ultimate responsibility for your output under ICH E6(R3) — has to qualify and monitor you.

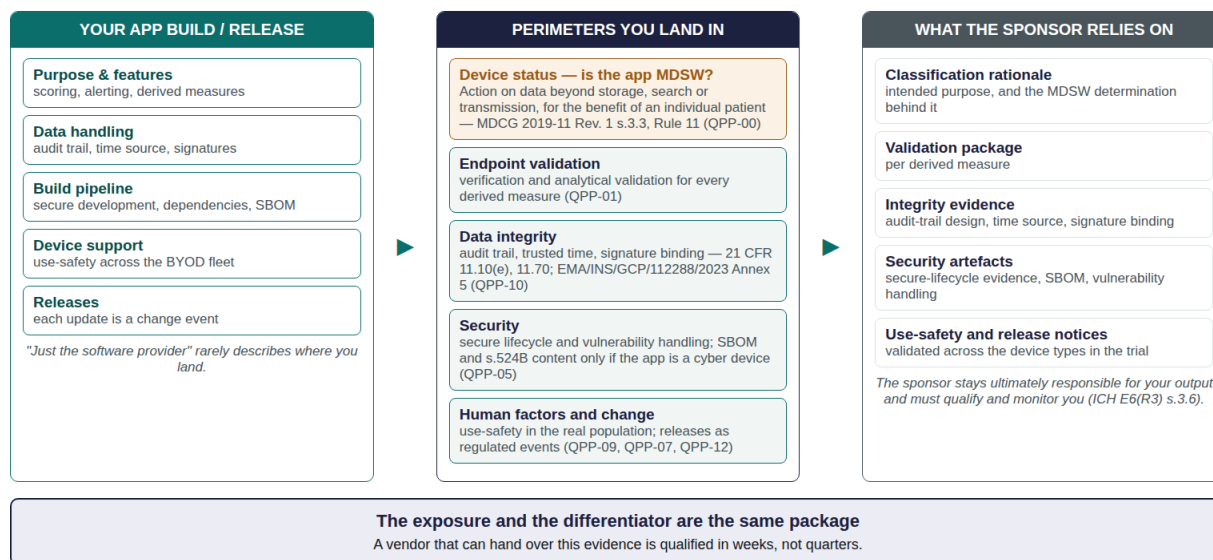
Build the package as you go. A vendor that can hand a sponsor the classification rationale, the validation evidence per derived measure, the integrity and security artifacts, the use-safety evidence across the device fleet and a release log is qualified in weeks rather than quarters. Retrofitting the same package at audit, with a study already enrolling, is the most expensive way to produce it.

¹ MDCG 2019-11 Rev. 1 (June 2025), "Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR", s.3.3 decision step 3 (software that "performs an action beyond storage, archival, communication, simple search, lossless compression" may be MDSW) and decision step 4 ("is the action for the benefit of individual patients?"; software only aggregating population data does not qualify); s.3.2 and s.6 (MDSW "may be placed on the market or put into service in its own right", and the type of interconnection does not affect qualification). Class follows MDR Annex VIII, Rule 11. Verified at https://health.ec.europa.eu/document/download/b45335c5-1679-4c71-a91c-fc7a4d37f12b_en?filename=mdcg_2019_11_en.pdf

² EMA, "Guideline on computerised systems and electronic data in clinical trials" (EMA/INS/GCP/112288/2023, adopted 7 March 2023), Annex 5 (A5.1, electronic clinical outcome assessment, including bring-your-own-device): "Validation should cover all device types and operating systems that will be used in the trial"; entry and save timestamps recorded as metadata; changes acknowledged by the data originator and documented in an audit trail. See also 21 CFR 11.10(e) (secure, computer-generated, time-stamped audit trails) and 11.70 (signature–record linking). https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-computerised-systems-and-electronic-data-clinical-trials_en.pdf

Your build and release choices are the sponsor's evidence — and the sponsor cannot produce them for you

Five product decisions land inside five regulated perimeters, and come back out as the package a sponsor has to hold.



Build it as you go. Retrofitting a validation package at audit is the most expensive way to produce it.

Illustrative. Which obligations apply turns on whether the app is a device and on the trial setup — a matter for structured assessment.

Figure 1 — Your build and release choices are the sponsor's evidence — and the sponsor cannot produce them for you.

1. The "just the software provider" framing understates where you land

This edition reads the series from the eCOA / ePRO vendor's seat. **ePRO — electronic patient-reported outcomes — is the participant-completed subset of eCOA, electronic clinical outcome assessment;** this edition uses eCOA for both except where the distinction matters. Where the app derives or interprets a measure, EU law calls it medical device software (MDSW); the US term for the same idea is software as a medical device (SaMD). One concept, two labels — this edition uses MDSW.

It is written for vendor leadership, product, quality and regulatory functions. Figure 2 sets out the EU qualification decision; section 3 sets out what the sponsor needs from you either way.

How this fits the full framework

This edition is keyed to Section 12 of the Regulatory Impact Assessment (QPP-00). It summarizes positions set out in full, with sources, in the numbered papers, which cluster for a vendor into three questions:

- **Is the app a device?** QPP-00 — Regulatory Impact Assessment (RIA): whether your software is MDSW in its own right. Where the app runs a model, QPP-04 — The AI/ML Overlay sets out the obligations that stack on top of the device ones.
- **Is the evidence sound?** QPP-01 — Endpoint Validation, QPP-10 — Data Integrity, QPP-05 — Cybersecurity and QPP-09 — Human Factors: the evidence package only you can produce.
- **Is it controlled over time?** QPP-07 — Change Control and QPP-12 — Vendor Qualification and Oversight: releases as regulated events, surfaced for the sponsor that must qualify and monitor you.

Regulatory basis

The sources behind this edition. The detail, and the rest of the citations, are in the numbered papers.

- **MDCG 2019-11 Rev. 1** (June 2025), ss.3.2, 3.3 and 6 — the decision steps that qualify software as MDSW, and MDSW placed on the market in its own right. Class under **MDR Annex VIII, Rule 11**.
- **EMA/INS/GCP/112288/2023** (adopted 7 March 2023), Annex 5 (A5.1) — eCOA and BYOD: validation across all device types and operating systems used in the trial; entry and save timestamps as metadata; changes acknowledged by the data originator and audit-trailed.
- **21 CFR Part 11**, ss.11.10(e) and 11.70 — secure, computer-generated, time-stamped audit trails; signature–record linking. **FDA**, *Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations: Q&A* (final, October 2024).
- **ICH E6(R3)**, Annex 1 s.3.6 and s.3.6.6 (Step 4, 6 January 2025; EU effective 23 July 2025) — service-provider agreements and oversight; ultimate responsibility resides with the sponsor.
- **FD&C Act s.524B** — the "cyber device" content, including the SBOM, where the app is a device that meets the three cumulative conditions.
- **Standards**: IEC 62304:2006 + A1:2015 (software lifecycle), IEC 62366-1:2015 + A1:2020 (usability engineering), IEC 81001-5-1:2021 (health-software security lifecycle), ISO 14971:2019 (risk management), ISO/IEC 27001:2022.
- **GDPR** Art. 28(2) and (4) — sub-processors require the controller's authorization and the same obligations flowed down.

Everything in this edition that is not attributed to a source above is qointa's professional assessment.

2. Four facts place you inside the regulated unit, not beside it

- **Your app can be the device.** MDSW is placed on the market in its own right, and the phone or tablet it runs on does not change that.
- **You own the evidence others rely on.** Validation, audit trail, change control and security of the app are yours.
- **You are also overseen.** The sponsor retains ultimate responsibility for your output under ICH E6(R3) and has to qualify and monitor you.³

³ ICH E6(R3), Annex 1 s.3.6 (agreements with and oversight of service providers) and s.3.6.6 (ultimate responsibility for trial-related activities, including reliability of the trial data, resides with the sponsor). Step 4, 6 January 2025; EU effective 23 July 2025.

- **Your releases are the trial's change events.** An update can move the app across a perimeter mid-study.

3. Seven perimeters apply, and you hold the evidence for most of them

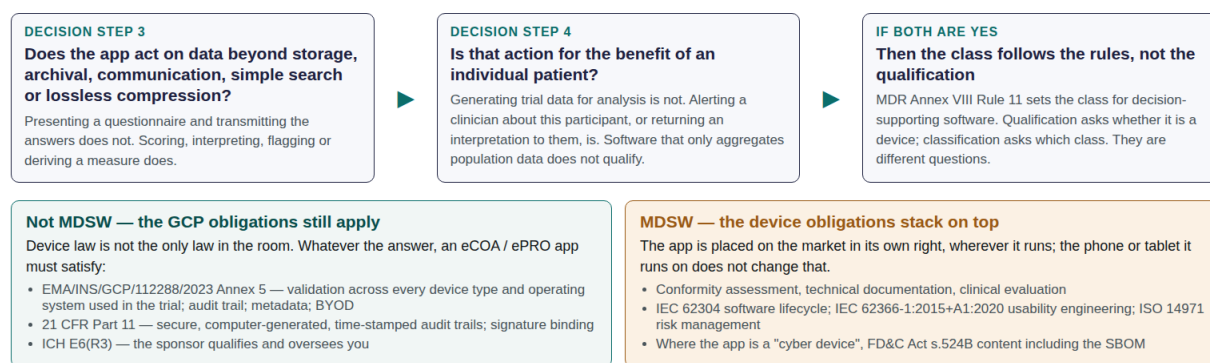
Your app sits at the center of seven regulatory perimeters, and most of them are built from evidence only you can supply. The last column is the artifact, not the aspiration. Where a row applies only if the app is a device, it says so.

Perimeter / topic	What it means for you	Paper	Vendor action / evidence
1 Medical device	Whether the app qualifies as MDSW under the MDCG decision steps — and, if it does, which class under Rule 11.	QPP-00	Determine the app's status on its actual functions; hold the intended-purpose statement and the rationale.
2 GxP and computerized systems	On-device audit trail, trusted time and signature binding.	QPP-10	Provide audit-trail design, time-source and signature-binding evidence.
3 Data protection and privacy	You are almost always a processor rather than a controller: the sponsor sets the purposes, and what you hold is the processing detail — hosting region, sub-processors and the route the data takes.	QPP-02	Supply the Article 28 processing terms, the sub-processor list, the hosting regions and the transfer mechanism for each country in scope.
4 Human factors and use safety	Formative and summative usability evaluation across the device types in the trial (IEC 62366-1:2015+A1:2020; FDA calls the summative stage human-factors validation testing) — a requirement in its own right.	QPP-09	Hand over formative and summative usability evidence for the population.
5 Configuration and change control	Releases as regulated events; surfacing changes for oversight.	QPP-07, QPP-12	Issue release notices and a change log the sponsor can act on.
6 Economic operator role	Where the app is medical device software placed on the market, you are its manufacturer. Where it reaches the trial through someone else's supply route, importer or distributor duties can attach to whoever moves it.	QPP-03	State which economic-operator role you hold in each market, and name the legal entity that holds it.

Perimeter / topic	What it means for you	Paper	Vendor action / evidence
7 Endpoint and protocol	Verification and analytical-validation evidence for any measure you derive (V3).	QPP-01	Supply an analytical-validation package for each derived measure.
Cross-cutting · Cybersecurity	Not one of the seven perimeters but a trigger family that fires across them: a secure development lifecycle and vulnerability handling for every app; an SBOM and the FD&C Act s.524B content only where the app is a "cyber device".	QPP-05	Run a secure development lifecycle (IEC 62304, IEC 81001-5-1:2021) and vulnerability management; supply an SBOM where the app is a cyber device.

Whether your app is a medical device turns on two questions, not on how you market it

MDCG 2019-11 Rev. 1 (June 2025) decision steps 3 and 4. Both must be answered yes before software qualifies as medical device software (MDSW).



Settle this before a sponsor asks, and hold the intended-purpose statement and the rationale behind it.

Illustrative summary of the MDCG decision steps. Qualification is a fact-specific assessment; the US boundary runs through FDA's general wellness and device software function policies instead.

Figure 2 — Whether your app is a medical device turns on two questions, not on how you market it.

4. Three blind spots turn up at vendor qualification

- **A "wellness" feature that does clinical work.** Marketing does not decide the question: scoring that is interpreted for an individual participant, or an alert routed to a clinician, can make the app MDSW whatever the app-store category says. In the US the line runs through FDA's general wellness and device software function policies instead.
- **A reference-device validation that misses the fleet.** The EU guideline expects validation to cover all device types and operating systems used in the trial; in a bring-your-own-device (BYOD) study the interface you tested is rarely the one every participant sees.
- **A sub-processor the sponsor never approved.** Hosting and analytics suppliers process trial data on your behalf, and GDPR Art. 28(2) and (4) require the controller's authorization before you engage them and flow the same obligations down. In qointa's assessment a connectivity carrier is usually not your sub-processor — it is a controller for its own traffic data — but the hosting and analytics chain is.

5. Six records make you easy to qualify

Six records turn a hidden obligation into an evidence package. Each one is a document a sponsor's vendor qualification asks for, and the checklist below is the same list in short form.

- **Determine the app's status early** — hold an intended-purpose statement and an MDSW determination against the MDCG decision steps before a sponsor asks.
- **Build the validation package as you go** — analytical-validation evidence for each measure, not retrofitted at audit.
- **Make integrity and security demonstrable** — audit trail, trusted time source, signature binding, a secure development lifecycle and, where the app is a cyber device, a current SBOM.
- **Evaluate use-safety on the real fleet** — formative and summative, across the device types and operating systems participants actually use.
- **Treat every release as a change event** — issue a notice and change log the sponsor can route into change control (QPP-07 — Change Control; QPP-12 — Vendor Qualification and Oversight).
- **Hold the instrument licenses and migration evidence** — the copyright position for each COA instrument and the evidence that the electronic version is equivalent to the one it replaces.

Vendor evidence checklist — what a sponsor needs to qualify you

The package a sponsor's vendor qualification asks for (Figure 1):

- **Determination rationale** — an intended-purpose statement and the MDSW determination behind it.
- **Validation package** — analytical-validation evidence for every measure the app derives.
- **Integrity proof** — audit-trail design, trusted-time source and signature binding.
- **Security artifacts** — secure-lifecycle evidence, vulnerability handling and, for a cyber device, a current SBOM.
- **Use-safety evidence** — formative and summative evaluation across the device types and operating systems in the trial, including the BYOD fleet.
- **Release notification** — a change log and release notices the sponsor can route into change control.

6. How qointa can help

qointa builds the evidence package described above with eCOA and ePRO vendors: the MDSW determination and its rationale, the validation plan across the device fleet, the audit-trail and time-source design, and the release notification that a sponsor can route into change control. We also sit on the sponsor side of vendor qualification, so the questions you will be asked are ones we have written.

Scope and status

This is a companion edition summarizing qointa's position-paper series from one stakeholder's seat, keyed to Section 12 of the Regulatory Impact Assessment (QPP-00). It summarizes positions set out in full, with sources, in QPP-01 — Endpoint Validation, QPP-05 — Cybersecurity, QPP-09 — Human Factors, QPP-10 — Data Integrity, QPP-07 — Change Control and QPP-12 — Vendor Qualification and Oversight. It is not legal advice; any specific position should be confirmed with qualified regulatory counsel.