

Regulatory Impact Assessment (RIA) for Devices and Systems in Clinical Trials

Why a device's role and triggers — not the hardware — determine whether an RIA is required

Prepared for	Any party in the device and system supply and operation chain — connected-device and phone manufacturers, sponsor, eCOA / ePRO vendor, logistics & provisioning, connectivity & device-management vendors, clinical-systems vendors, CRO and sites (full set in Section 12).
Subject	Why every device and system a trial relies on — from a wearable or home instrument to the phone or gateway that carries its data and the platform that receives it — requires a Regulatory Impact Assessment, and how to scope one proportionately, per stakeholder.
Status / Date	Final — 1 September 2026
Version	1.0
Prepared by	Rudiger Mees

Reading this paper in context

This is **QPP-00 — Regulatory Impact Assessment (RIA)**, the anchor of the qointa **Digital Health Technologies (DHT) in Clinical Trials** series. It sets out the core position — **assess rather than assume** — and the three instruments the rest of the series keys to:

- **The role scale** (Section 6) — five rungs from passive carrier to MDSW / SaMD execution.
- **The triggers** (Section 7) and the **Trigger Register** that holds them — developed in QPP-08 — Trigger Register.
- **The lifecycle** (Section 8) — baseline, then re-assessment on material change.
- **Section 12 — What this means for each stakeholder** — applied party by party in the fourteen Stakeholder Editions S01–S14.

The Primer and the Series Overview introduce this paper; QPP-01 to QPP-24 develop the individual perimeters it names (for example QPP-03 — Economic-Operator Roles, QPP-04 — The AI/ML Overlay, QPP-05 — Cybersecurity, QPP-10 — Data Integrity).

Executive summary

Every device and system a trial relies on needs a Regulatory Impact Assessment (RIA) — and for most deployments that assessment is short and returns minimal controls. “It’s just a phone,” “it’s just the modem,” “it’s already a cleared device” are conclusions the assessment can reach; none is an exemption from performing one. A device’s regulatory weight is set by what it does in the protocol — its role and the triggers it activates — not by its form factor.

- **“No RIA needed” is a conclusion, not a starting point.** Only the assessment can reach it; skipping the assessment leaves the risk undetermined and the decision undocumented.
- **Function, not hardware, sets the obligations.** The same smartphone can be a passive carrier in one study and a measurement instrument or medical-device-software host in another; the same wearable can be a cleared device used exactly as labelled, or an endpoint instrument whose output must be validated for this protocol.
- **“Not a device” does not mean “no controls.”** FDA’s 2023 DHT guidance expects verification and validation regardless of whether the tool meets the device definition.
- **The RIA protects the stakeholder, not just the regulator.** For most deployments it legitimately returns minimal or standard controls — the light-touch outcome most parties want, reached defensibly and on record.
- **It is proportionate and per-stakeholder.** Effort scales to the risk found, one party’s assessment does not discharge another’s, and the analysis is re-run on material change — it is a lifecycle, not a one-time gate.

The RIA decision framework: four recorded steps

1	Establish the role	Passive carrier ► data relay ► eCOA / ePRO / eConsent host ► measurement instrument ► MDSW / SaMD execution. Regulatory weight rises along this five-rung scale (Section 6).
2	Test the triggers	Own-sensor measurement, endpoint feed, medical purpose, locked-down configuration, eConsent, GCP source data, safety alerts, app / OS / firmware / AI updates, and device heterogeneity (the nine triggers in Section 7).
3	Record the decision	Minimal ► standard ► full device and GxP controls, scoped to the responsible stakeholder and documented with its rationale.
4	Re-assess on change	Re-run at baseline and on any material change — software, firmware or OS updates, new endpoints, a new vendor or route, or a new country — recorded in the Trigger Register (QPP-08 — Trigger Register).

How this differs from the guidance it builds on

This framework does not replace FDA, EMA or ICH expectations — it **operationalizes** them. Where the source guidance states *what* is expected (fit-for-purpose evidence, sponsor accountability, change control), the RIA turns it into a **per-stakeholder, lifecycle decision tool**: who assesses what, against which framework, at baseline and on every material change.

1. Every party in the device chain must assess its own footprint

Trial teams often treat the devices and systems used in their studies — the participant's smartphone, the provisioned handset, the cellular gateway, the wearable that is “already a device” — as commodity hardware that “does not need a Regulatory Impact Assessment (RIA)” — by which this series means a structured, recorded determination of which regulatory obligations a device's use in a specific study attracts, and which party carries each of them. This paper sets out why that exemption cannot be assumed. For every party in the device supply and operation chain, it explains why “it's just a phone” — the most common form of the claim — cannot be adopted as a default exemption, and why a proportionate RIA, scoped to each stakeholder's role and the obligations that party actually carries, is the correct and defensible way to reach a controls decision, including the decision that only minimal controls are needed.

Because each party carries a different footprint, **one stakeholder's assessment does not discharge another's**. A sponsor's RIA does not settle the position of its eCOA, connectivity or device-management vendor, and vice versa. The assessment is therefore framed per stakeholder, against the specific study setup.

It is addressed to everyone whose actions affect how a device or system is bought, configured, kitted, connected, distributed, used as a data source, updated or retired across its life — among them the device manufacturer, the sponsor, the eCOA / ePRO provider, the logistics and provisioning vendor, the CRO and the sites, with the wider set of parties in Section 12.

The scope is every device or system a trial relies on in a non-investigational capacity — used in an auxiliary role to run the trial rather than as the object of investigation: dedicated medical devices, wearables and biosensors, home and point-of-care instruments, smartphones and tablets whether provisioned or the participant's own, connectivity gateways, and the eCOA, eConsent and clinical-systems platforms that receive what they produce. The smartphone recurs as the example because it is the most common case and because, even where it measures nothing, it usually carries another device's data to the sponsor. Where a device is itself the object of the investigation, it sits in its own clinical-investigation pathway. For everything used to conduct the trial rather than to be studied by it, qointa's position is that the assessment is required, not optional. Where a device is already a medical device, the assessment turns not on whether it qualifies — that is settled — but on what its use in this specific setup requires and which stakeholder carries it.¹

2. One device can carry several sets of obligations at once

One device can sit inside several regulatory perimeters at the same time. The single word “phone” — or “wearable,” or “gateway” — can conceal a medical-device-software host, an electronic-records system, a data-protection processor, an economic-operator artifact and an AI system at once — obligations that stack rather than substitute. Figure 1 shows the perimeters a single device can occupy. This paper calls each of them a perimeter; the triggers in Section 7 are grouped by the seven regulatory perimeters the series uses — medical-device, GxP, data-protection, human-factors, configuration, economic-operator and protocol-design. AI and cybersecurity are frameworks that cut across the medical-device and GxP perimeters rather than perimeters of their own.

¹qointa's position, consistent with the sponsor's responsibility under ICH E6(R3) section 3.6 to ensure that the systems, equipment and tools used in a trial are fit for purpose and produce reliable data, whether or not they are the investigational product. On the device side, see MDCG 2022-10, Q&A on the interface between Regulation (EU) 536/2014 (CTR) and Regulation (EU) 2017/746 (IVDR), May 2022 — confirming that an in vitro diagnostic device or assay used in a clinical trial must comply with the IVDR even where it is not itself under investigation.

One device, several perimeters: the obligations stack rather than substitute

One device — a wearable, a home instrument, a smartphone, a tablet or gateway, an eCOA platform — can carry six sets of obligations at once. Each applies on its own terms; none displaces another.

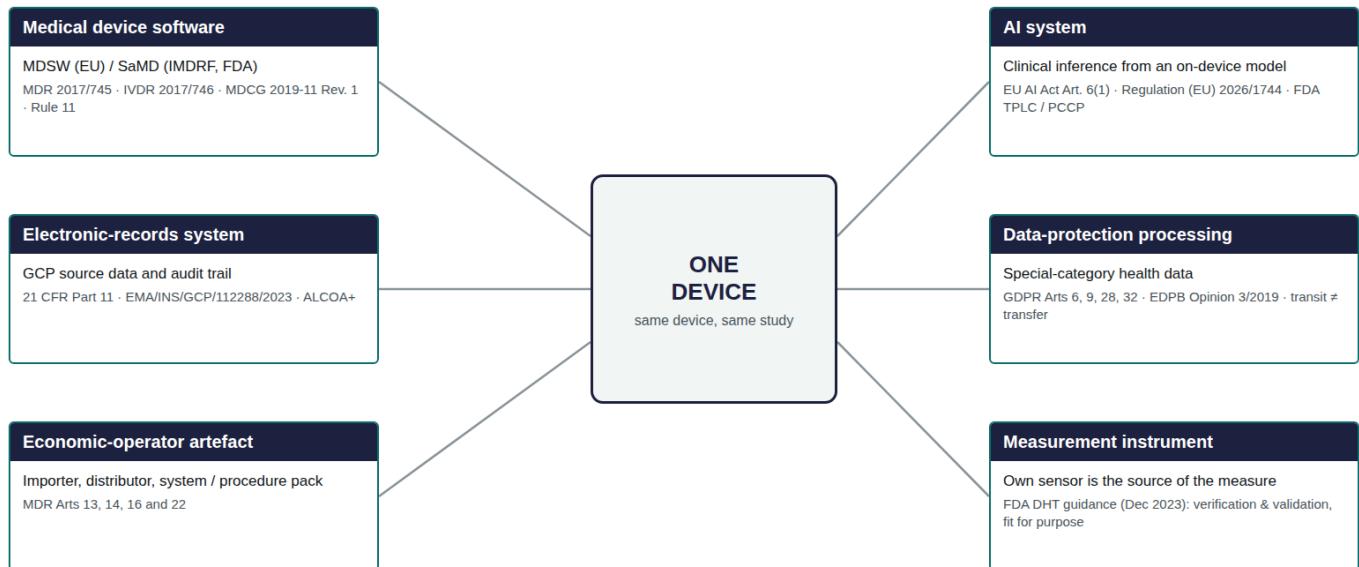


Figure 1. One device, several perimeters — the obligations stack rather than substitute.

The four core principles

- **Function, not form factor.** Regulatory status follows what the device does in the protocol, not the fact that it is “a phone,” “a modem” or “already a cleared device.”
- **“Not a medical device” is not the end of the analysis.** Verification, validation and fit-for-purpose evidence apply regardless of the device definition.
- **“No RIA needed” is an output, not an input.** The exemption is what the assessment produces — it cannot be the reason to skip one.
- **Proportionate and per-stakeholder.** Effort scales to risk, duties can be inherited by operation of law (MDR Article 16 for parties that modify or relabel a device, Article 22 for systems and procedure packs), and the scope is every non-investigational tool.

3. “It’s just the hardware” is a conclusion the assessment reaches, not a reason to skip it

An illustrative scenario

A sponsor running a remote study treated the participant handsets as ordinary BYOD phones and skipped a formal assessment. Mid-inspection, the agency noted that a breathing-test feature used the phone’s own microphone to derive a secondary endpoint — a measurement function that pulled the app toward medical-device-software territory. There was no verification record, no documented data flow and no rationale on file. The fix was retrospective: validation after the fact, a protocol amendment, and weeks of avoidable delay. None of it was caused by the phone. All of it was caused by **not assessing the phone**.

Illustrative composite — not a specific study.

The usual reasoning is that the hardware — a phone, whether the participant's own (BYOD) or sponsor-provisioned; a cellular gateway; a consumer wearable — is general-purpose, commercial-off-the-shelf equipment, and therefore falls outside regulatory assessment. In the large majority of deployments the device is indeed a non-investigational tool that carries the study but is not itself the object of investigation. The difficulty is that “merely carries the study” is itself a classification. The only way to confirm it applies to a given deployment is to assess that deployment's role and triggers. The exemption stakeholders want is the output of an RIA, not a reason to skip one.

Where a device really is a passive carrier — transporting or displaying data that originates elsewhere, measuring nothing itself, running no medical-purpose software — the controls that follow are light. But “it is just a phone” cannot be the assumption that ends the inquiry. At most it is a conclusion reached after one.

The duty to assess attaches to what the device does, not to the hardware. FDA's digital-health guidance expects verification and validation “regardless of whether the DHT meets the definition of a device.” ICH E6(R3) expects the computerized systems used in a trial to be “fit for purpose” and recorded with their validation status. Neither carves out consumer hardware.

The position also collapses the moment any trigger is present — the device's own sensor sourcing a measurement, an app performing a medical function, a feed into an endpoint, a locked-down configuration, eConsent, GCP source data, or an on-device AI model or update. None of these is exotic. Nor does “just a phone” survive even at the floor: a true carrier still warrants capturing the software, firmware and operating-system versions in use and a documented data flow. So “minimal” never means “nothing.”

The practical point is one of evidence, not burden. Declining to assess does not make the risk smaller; it leaves it undocumented. **“We believed it didn't apply” is the weakest position to defend at inspection; “we assessed it and recorded why it is minimal” is the strongest.** The assessment is not an obstacle to the light-touch outcome the claim is reaching for — it is how that outcome is earned and made defensible.

4. No two device deployments occupy the same regulatory position

There is no single “phone deployment” or “wearable deployment” to which a blanket rule could apply. Setups differ along independent dimensions, and each combination sits in a different regulatory position.

- **How the device reaches the participant.** It may be the participant's own device (BYOD) or a unit provisioned and locked down by the sponsor or a delegate — placing the controlled state in different hands.
- **How the device is procured.** A medical device may be bought directly from the manufacturer, or from its authorized importer or distributor — and the purchaser may be the sponsor, the eCOA / ePRO vendor or the logistics vendor.
- **How it is connected and managed.** The eSIM, data-plan or gateway provider determines where traffic routes — a security-in-transit and data-localization question, which becomes a cross-border transfer only where a third-country party receives or accesses the data — while the device-management (MDM) vendor controls the locked-down state — a layer most blanket views overlook entirely.
- **Where it operates.** Data-residency rules, Member-State differences in how device rules are applied to trials (in qointa's experience), and which device and AI regimes apply at all turn on geography. The same device can sit differently from one country to the next.

These choices are not interchangeable in regulatory terms. Frameworks such as the EU MDR assign **distinct obligations** to manufacturers, authorised representatives, importers, distributors and the persons

who assemble systems or procedure packs (Articles 10–16 and 22).² The route by which a device enters a study therefore changes where those obligations sit and how the chain of accountability is evidenced. Two studies using what appears to be the same device can occupy **entirely different regulatory positions** depending on who bought what, from whom, in which role, where, and for what use — which is precisely why a setup cannot be exempted in the abstract.

The three setups this series uses as its running examples show the spread. A sponsor-provisioned smartphone running the eCOA diary sits on rung 3 of the role scale (Section 6), with the configuration and economic-operator perimeters engaged because the sponsor owns and ships the handset. A wrist-worn wearable paired to the participant's own phone splits: the wearable is a measurement instrument (rung 4) whose output must be validated for this protocol, while the phone is a data relay (rung 2) the sponsor does not control, so an operating-system update is a trigger it can only detect. A home spirometer paired to a provisioned cellular gateway puts a cleared medical device at rung 4 and a sponsor-controlled relay at rung 2 — the economic-operator and configuration duties fall on the sponsor or its logistics vendor for both. Same series, three different controls decisions.

5. Obligations attach to function, so the hardware label settles nothing

Regulatory obligations attach to function, not to the object. Several points follow.

- **Status is read from the context of use.** A phone that records a 6-minute walk via its accelerometer is doing something different, in regulatory terms, from one that displays a reminder — even though it is the same phone; a wearable whose step count feeds a secondary endpoint is doing something different from one worn for engagement — even though it is the same wearable.
- **The “general-purpose device” exclusion is conditional.** “It’s just a phone” — or just a tablet or gateway — is really a claim to a general-purpose computing-platform exclusion. In the US that exclusion is explicit: FDA “does not consider mobile platform manufacturers to be medical device manufacturers just because their mobile platforms could be used to run a mobile medical app regulated by FDA.” In the EU the same result follows from the manufacturer’s intended purpose under the MDR, not from a hardware exclusion. Either way the exclusion is narrow, and in qointa’s assessment it is forfeited the moment the device is configured, modified or instrumented for a medical, regulated-record or controlled-platform purpose — which is much of what trial use does.
- **The app can be the device.** Software intended for a medical purpose can be medical device software in its own right — MDSW in EU terms, software as a medical device (SaMD) in IMDRF and FDA usage — irrespective of the consumer hardware it runs on.³ The hardware label does not shield the software function.
- **Evidence is required even when it is not a device.** Fit-for-purpose verification and validation obligations apply to data-generating digital tools whether or not they meet the device definition. “Not a device” therefore does not equal “no controls,” and does not equal “no assessment.”

6. The device’s role sets its regulatory significance

The same device occupies different rungs depending on what the protocol asks of it. Its regulatory significance rises with the rung (Figure 2), which also places the series’ three running examples on the scale.

² ICH E6(R3), Good Clinical Practice (Step 4, 6 January 2025): computerised systems used in clinical trials should be fit for purpose; a record of important computerised systems and their validation status is expected.

³ Routing through a third country is transit, not a transfer: ICO, “What is an international transfer of personal information?” (“Transfer doesn’t mean the same as transit ... but the controller must consider the security of the information while it’s in transit”); EDPB Guidelines 05/2021 on the interplay between Article 3 and Chapter V GDPR (a transfer requires an exporter disclosing or making data available to an importer in a third country).

Regulatory weight rises with the device's role, not with its hardware

The same device occupies a different rung in every study; the rung sets the controls the assessment will require. Examples from the three common setups used across the series.

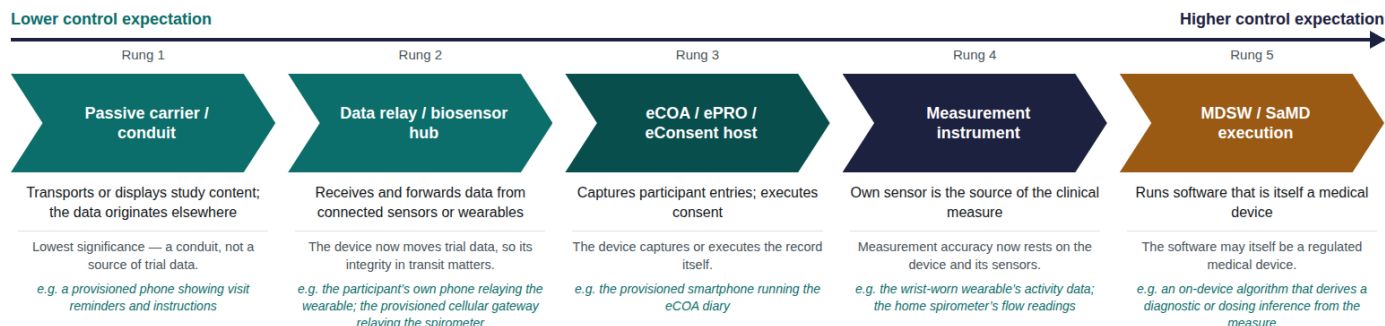


Figure 2. The role scale — regulatory weight rises with the device's role, not with its hardware; the five rungs are those used throughout the series, with the three running examples placed on them.

Illustrative only — this scale shows how significance escalates with the device's role; it is not a menu to self-select from. Placing a specific setup on it is a matter for structured assessment.

7. Nine triggers move a deployment up the scale

Each “yes” below moves a deployment up the scale. These are the questions an assessment exists to ask in a structured, recorded way — rather than to assume the answers to.

If this is true of the deployment...	...the regulatory weight rises because
The device's own sensor is the source of a clinical measurement (not just a relay).	Measurement accuracy now depends on consumer hardware.
The output feeds a primary or secondary endpoint.	Endpoint reliability has to hold up, not be assumed.
The app performs a medical purpose (diagnosis, prediction, dosing, triage, alerts).	The software may be MDSW / SaMD in its own right.
The device — handset, tablet or gateway — is provisioned and locked down by the sponsor or a delegate.	The sponsor now owns part of the controlled configuration.
The device executes informed consent (eConsent).	Consent integrity and the surrounding records are at stake.
Records are GCP source data subject to 21 CFR Part 11 and the EMA computerized-systems guideline (EMA/INS/GCP/112288/2023).	Data-integrity and electronic-record expectations attach.
A safety signal or alert is generated or surfaced to a participant or site.	Patient-safety risk raises both device and oversight duties.
App, OS, firmware or on-device AI updates can alter the validated measurement mid-study.	The validated state can drift after it was established.

If this is true of the deployment...	...the regulatory weight rises because
Device, firmware or OS heterogeneity — BYOD or a mixed provisioned fleet — affects comparability of the measure.	Equivalence across devices cannot simply be presumed.

Illustrative only — these nine examples are drawn from qointa's Trigger Register (QPP-08 — Trigger Register), which spans seven regulatory perimeters (medical-device, GxP, data-protection, human-factors, configuration, economic-operator and protocol-design) and are not a self-administering checklist. Which triggers fire, and what follows, is a matter for structured evaluation of the specific setup.

8. The assessment has a lifecycle, not a start date

The triggers that decide whether an RIA is needed at the outset do not fall silent once the study opens. A deployment that is a passive carrier on day one can acquire a measurement or medical-device function later, without anyone choosing to move it. The assessment is therefore performed at two points: once at **baseline**, before the device is relied upon, and again **whenever a material change** disturbs the basis the baseline rested on.

FDA's DHT guidance expressly addresses changes to a DHT during a study (section IV.H.4),⁴ and E6(R3)'s risk-based, quality-by-design approach treats the assessment as iterative rather than a single pre-study sign-off (section 3.9).⁵ In qointa's assessment a **living RIA** is how a sponsor meets what these frameworks already expect — not an additional burden this paper invents.

The assessment is a lifecycle: a baseline, then re-assessment at every material change

The loop repeats until the study closes. A one-time exemption goes stale the first time an update, endpoint, vendor, route or country changes.

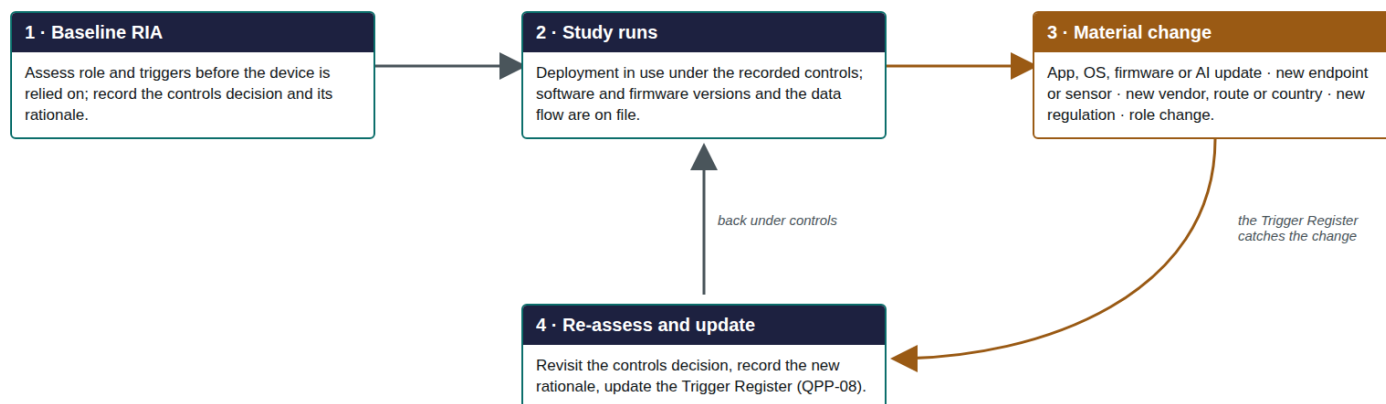


Figure 3. The assessment lifecycle — a baseline, then re-assessment at every material change, until the study closes.

Material change triggers re-assessment (Figure 3). The kinds of event below map to the same regulatory perimeters the triggers are drawn from; the Trigger Register holds the study-specific list.

- **Configuration and technical change.** An app, OS or firmware update, a new MDM policy, or a different handset, wearable or gateway model entering the fleet — any of which can alter validated behavior.
- **Protocol change.** A new or amended endpoint, a sensor added to the setup, the introduction of eConsent, or a change in how a measure is captured.

⁴ Regulation (EU) 2017/745, Articles 10 (manufacturer), 11 (authorised representative), 13 (importer), 14 (distributor), 16 (cases in which obligations of manufacturers apply to importers, distributors or other persons) and 22 (systems and procedure packs).

⁵ FDA, Policy for Device Software Functions and Mobile Medical Applications — Guidance for Industry and FDA Staff (28 September 2022), section V. <https://www.fda.gov/media/80958/download>

- **Supply-chain and operational change.** A change of provisioning, logistics or connectivity vendor, a different procurement route, or the addition of a country.
- **Data-flow change.** A shift in where traffic routes or data resides, or a new cross-border transfer.
- **Regulatory-environment change.** A new or revised AI regime, fresh guidance, or a shift in how a classification question is read in a relevant jurisdiction.
- **Role change.** A party taking on provisioning, kitting or import such that it becomes a manufacturer, importer or distributor by operation of law (MDR Articles 13, 14 and 16).

Illustrative only — these categories show the kinds of change that reopen the assessment; they are not an exhaustive register. Whether a given change is material, and what it requires, is a matter for structured evaluation of the specific setup.

9. The frameworks converge: evidence follows function, whether or not the tool is a device

The relevant frameworks converge on a single point: obligations follow the **function and risk** of the digital tool, and fit-for-purpose evidence is expected even where the tool is not formally a device.

- **ICH E6(R3) Good Clinical Practice**⁶ — Step 4 on 6 January 2025, effective in the EU from 23 July 2025, published by FDA in September 2025 — takes a media-neutral, fit-for-purpose, risk-based (quality-by-design) approach, with expanded expectations for computerized systems, digital health technologies, electronic source data and eConsent. Annex 2, on decentralized elements, pragmatic trials and real-world data sources, reached Step 4 on 3 June 2026 and takes effect in the EU on 15 January 2027. Under section 3.6, “the ultimate responsibility for the sponsor’s trial-related activities, including ... the reliability of the trial data, resides with the sponsor,” however activities are transferred.
- **FDA DHT guidance**⁷ (final, December 2023) — a DHT is **defined by its function**; sponsors should select fit-for-purpose DHTs and address verification and validation (section IV.C) **regardless of whether the DHT meets the device definition**. It expressly addresses participants’ own devices (section IV.A) and changes during a study (section IV.H.4) — the direct answer to “it isn’t a device, so nothing applies.”
- **EU MDR 2017/745 and MDCG 2019-11 Rev. 1.** Software for a medical purpose can be MDSW in its own right, irrespective of the consumer hardware; qualification and classification (commonly Rule 11) must be assessed. Where the function is diagnostic from a specimen, the parallel pathway is the IVDR (2017/746), not the MDR — which the assessment must determine rather than presume.⁸⁹
- **IMDRF SaMD framework.** Where the device executes software as a medical device, risk is categorized by the significance of the information provided and the healthcare situation, which drives the rigor expected.
- **AI-specific frameworks.** Where the device — or the phone it pairs with — runs an AI/ML model producing a clinical inference, AI regulation attaches in addition to the device rules. The EU AI Act (Regulation (EU) 2024/1689) classifies an AI system as high-risk under Article 6(1) only where two cumulative conditions hold: it is a product, or a safety component of a product, covered by the Annex I legislation — which includes the MDR and IVDR — and that product requires third-party conformity assessment under that legislation. AI inside a self-declared Class I device is therefore not high-risk by this route. Regulation (EU) 2026/1744 (the Digital Omnibus on AI, in force 27 July 2026) moved the

⁶ Regulation (EU) 2017/745, Article 2(1) (definition of “medical device” by the manufacturer’s intended purpose) and recital 19 (software for general purposes is not a medical device).

⁷ MDCG 2019-11 Rev. 1 (June 2025), Guidance on qualification and classification of software in Regulation (EU) 2017/745 and Regulation (EU) 2017/746; IMDRF/SaMD WG/N10FINAL:2013, Software as a Medical Device: Key Definitions.

⁸ FDA, Digital Health Technologies for Remote Data Acquisition in Clinical Investigations (final guidance, December 2023), section IV.H.4.

⁹ ICH E6(R3), section 3.9 (sponsor quality management, risk-based approach).

device-embedded high-risk obligations to 2 August 2028 and the Annex III obligations to 2 December 2027. The US addresses AI-enabled devices through FDA's total-product-lifecycle approach and Predetermined Change Control Plans under section 515C of the FD&C Act (final guidance December 2024, re-issued 18 August 2025) — which apply to marketed device software functions, not to investigational devices. This is the fastest-moving perimeter of all. In qointa's assessment, AI increasingly enters not through the trial app but through the device's own OS or assistant layer, so a model can appear with no protocol decision behind it — the silent-update problem, one layer down.

- **Data integrity & computerized systems.** 21 CFR Part 11 (US) and the EMA Guideline on computerised systems and electronic data in clinical trials (EMA/INS/GCP/112288/2023) bring validation, audit trail, access control and electronic-signature expectations to any system holding GCP records, with ALCOA+ as the baseline. The two jurisdictions diverge on the device itself: FDA locates electronic source data from a DHT in the durable electronic data repository and “does not intend to inspect individual DHTs for source data verification,” whereas the EMA guideline expects device-side controls (Annex A4 security; Annex A5 specific systems) — so the record's integrity from capture to repository remains the sponsor's to evidence in both.
- **Decentralized-trial guidance.** FDA's Conducting Clinical Trials With Decentralized Elements (final, September 2024)¹⁰ and the HMA/EC/EMA Recommendation paper on decentralized elements in clinical trials (Version 02, 1 October 2025)¹¹ both treat participant-side devices as a deliberate design choice. The EU paper expects decentralized elements likely to have a significant impact on scientific validity, data integrity, benefit-risk ratio or participants' rights to be considered in a **specific and documented risk-benefit assessment**. The RIA is a practical way to meet that expectation for the device layer.
- **Cybersecurity.** A connected device holding GCP source and special-category health data — a handset, a wearable, a gateway — is an attack surface. Where the device or app is a medical device, the EU addresses this under MDCG 2019-16 Rev. 1 and the US under section 524B of the FD&C Act, which defines a “cyber device” by three cumulative elements: it includes software validated, installed or authorized by the sponsor; it can connect to the internet; and it contains technological characteristics that could be vulnerable to cybersecurity threats. Where it is not a medical device, the EU basis is GDPR Article 32 (security of processing). This feeds the lifecycle point: the security patches that cannot be refused are the updates most likely to disturb the validated state.
- **Human factors and accessibility.** Where the participant operates the device, usability is part of data quality: usability engineering (IEC 62366-1:2015 + A1:2020) bears on whether entries are captured as intended, and accessibility and the digital divide bear on equity of access and the representativeness of the data. Both sit within the DHT and decentralized-trial guidance.
- **Data protection.** Trial data on a participant-side device are special-category health data (GDPR Article 9). The legal basis for processing them is usually not consent — Article 6(1)(c), (e) or (f) with Article 9(2) (i) or (j) — and trial consent under the Clinical Trials Regulation is not GDPR consent; withdrawal from the trial does not by itself trigger erasure (CTR 536/2014 Article 28(3); GDPR Article 17(3)). A vendor that processes the data on the sponsor's behalf needs an Article 28 processing contract; and routing through a third country is transit, not a transfer, until a third-country party receives or accesses the data.

Key frameworks at a glance: each expects fit-for-purpose evidence, whatever the device's status

¹⁰ ICH Harmonised Guideline E6(R3), Good Clinical Practice — Principles and Annex 1: Step 4 6 January 2025; effective in the EU from 23 July 2025; published by FDA (Federal Register) 9 September 2025. Annex 2: Step 4 3 June 2026; effective in the EU from 15 January 2027.

¹¹ FDA, Digital Health Technologies for Remote Data Acquisition in Clinical Investigations (final guidance, December 2023), docket FDA-2021-D-1128.

Framework	What it governs	Core expectation for a device-based trial
ICH E6(R3) GCP	Sponsor accountability, quality-by-design, data governance	Ultimate responsibility for the reliability of trial data resides with the sponsor (s.3.6); the tools used must be fit for purpose, whatever the device's status.
FDA DHT guidance (2023)	Digital health technologies for remote data acquisition	Verification, validation and fit-for-purpose evidence expected even where the tool is not a device; updates must be handled.
FDA decentralized-elements guidance (2024)	Trials with decentralized elements	Participant-side devices are a deliberate design choice with defined sponsor and investigator duties.
EU MDR 2017/745	Medical devices and medical-device software	Software for a medical purpose can be MDSW (commonly Rule 11); economic-operator duties apply (Arts 13, 14, 16 and 22).
EU IVDR 2017/746	In vitro diagnostics and assays	Diagnostic-from-specimen functions follow the IVDR; even a non-investigational IVD in a trial must comply (MDCG 2022-10).
EU AI Act 2024/1689	AI systems	AI that is, or is a safety component of, a device requiring third-party conformity assessment is high-risk (Art. 6(1)); device-embedded obligations apply from 2 August 2028 (Regulation (EU) 2026/1744).
21 CFR Part 11 / EMA/INS/GCP/112288/2023	Computerized systems and electronic records	Validation, audit trail, access control and ALCOA+ for any system holding GCP records.
Cybersecurity — MDCG 2019-16 Rev. 1 / s.524B FD&C Act	Device and data security	Security of processing (GDPR Art. 32 where the device is not a medical device); the patches that cannot be refused are the updates most likely to disturb the validated state.
GDPR 2016/679 / EDPB Opinion 3/2019	Personal and special-category health data	Legal basis under Arts 6 and 9 (not consent); Art. 28 processor contract; withdrawal ≠ erasure; transit ≠ transfer; security in transit (Art. 32).

2026–2028 outlook: the perimeters are converging

The period to 2028 tightens the case for assessing rather than assuming, because the AI, DHT and decentralized-trial regimes are moving toward each other:

- **AI Act, device-embedded high-risk — from 2 Aug 2028.** Regulation (EU) 2026/1744 (the Digital Omnibus on AI) extended the runway, not the obligation; conformity work has to start well before the date.
- **E6(R3) Annex 2 (decentralized elements, pragmatic trials, real-world data sources) — Step 4 on 3 June 2026, effective in the EU from 15 January 2027.** Its expectations for participant-side devices and real-world data sources now have a date.
- **MDR / IVDR targeted revision — Commission proposal COM(2025) 1023 (December**

2025); status: proposal. It would change how the device regulations and the AI Act overlap — another reason to track classification, not freeze it.

- **On-device AI by default.** Assistant and OS-level models arrive through routine updates, pulling AI obligations into deployments that never chose them.

*The practical implication is the same one this paper makes throughout: a **living RIA** absorbs these shifts as material-change events, where a one-time exemption simply goes stale.*

10. The assessment scales to the risk it finds

Whether controls are needed — and how far they extend — is itself the **output** of the assessment, not something knowable in advance of it. That is what makes the assessment inherently proportionate: it weighs only what the deployment's role and triggers warrant, fully in keeping with E6(R3)'s risk-based, quality-by-design approach and the fit-for-purpose principle.

Note the asymmetry.

A light-touch result is both valid and common. Where a device is genuinely a passive carrier, the assessment records exactly that and closes the question. Most parties who question the assessment want exactly that result — the assessment is simply how the result becomes defensible rather than assumed. Declining it does not deliver the same outcome; it leaves the position unestablished.

The objection answered.

The real objection is rarely that risk is absent; it is that assessment feels like overhead on commodity hardware. The answer is that the work scales to the risk it finds. A genuine passive-carrier deployment produces a short record and closes the question. Only deployments that actually carry measurement, consent or medical-device functions attract real effort — and even there the assessment is modest beside the retrospective validation, protocol amendments or unusable data that a perimeter crossed unnoticed can cost.

What it looks like in practice.

A proportionate RIA is not a heavy artifact. It takes the study setup as its input — the device's role on the scale in Section 6, the triggers in Section 7, the procurement and connectivity route, and the countries involved — tests it against the applicable frameworks, and records a controls decision with its reasoning. Inside the sponsor it is owned jointly across QA / GCP compliance, Regulatory Affairs, computerized-system validation and the study's project management. Even the lightest outcome has a floor: a pure carrier still warrants capture of the software, firmware and OS versions in use and a documented data flow, so “minimal controls” means a recorded baseline, not the absence of one.

11. Skipping the assessment defers the cost; it does not remove it

Skipping the assessment does not remove the risk; it defers it to a point where it is harder and more expensive to fix. The table sets out the main exposures when a deployment goes unassessed — how likely each is and its impact (qointa's judgment), what it leads to, and **how a proportionate RIA heads it off**.

If the assessment is skipped	Likelihood	Impact	What it leads to	How the RIA mitigates it
Undocumented assumption at audit	High	High	“We believed it didn't apply” is the weakest position at inspection.	A recorded rationale converts a belief into defensible evidence.

If the assessment is skipped	Likelihood	Impact	What it leads to	How the RIA mitigates it
Endpoint left unsupported	Medium	High	No V&V evidence if a sensor-derived measure is challenged.	Triggers the verification and validation a measurement role requires.
Mis-qualified MDSW	Medium	High	An app that is really SaMD running without device controls.	Forces qualification / classification before reliance.
Economic-operator duties inherited	Medium	High	Manufacturer / importer / distributor status by law (MDR Art. 16); kitting can bring the assembler within Art. 22.	Maps the supply route and flags inherited operator duties early.
Data-integrity gaps	Medium	High	Part 11 / EMA guideline / ALCOA+ failures on GCP source data.	Scopes audit trail, access control and validation up front.
Data-protection exposure	Medium	High	Special-category data, residency and transfer duties left unmet.	Surfaces residency and cross-border transfer in the connectivity review.
Silent trigger mid-study	High	Medium	A routine app or OS update crosses a perimeter unnoticed.	The Trigger Register catches the change as it happens.
Late remediation	Medium	High	Retrospective validation, amendments, or data unusable for submission.	Moves the work to baseline, where it is cheapest to do.
End-of-life left open	Medium	Medium	Source or health data lost or stranded at retirement.	Builds retirement and data-retention into the controls decision.

Across all of these, ultimate responsibility for the reliability of the data resides with the sponsor under ICH E6(R3) section 3.6, however much is transferred — so the cost ultimately lands on the sponsor even where the work sat with a vendor.

Why this is not hypothetical

In qointa's inspection experience, computerized-system and data-integrity findings recur in GCP inspections, and FDA (BIMO), EU competent authorities and MHRA have widened their attention to digital health technologies and decentralized elements as remote data capture has become routine. The specific failure modes above — missing validation evidence, undocumented data flows, unmanaged updates — are exactly the observations that surface when a digital tool is relied on without a recorded assessment. A proportionate RIA prevents them at a fraction of the cost of remediation.

12. What this means for each stakeholder: obligations follow the configuration each party owns

The chain reaches well beyond the obvious parties. Each of the following can inherit obligations by operation of the configuration it owns — often with **no contract clause assigning them**. Each row is developed in the corresponding Stakeholder Edition (S01–S14).

Stakeholder	Why this matters to you
Phone manufacturer / OEM	Hardware specification, sensor performance and change-notification feed the V&V and fit-for-purpose evidence others rely on.
Connected-device manufacturer	Where a phone or gateway bridges to a CGM, ECG patch, spirometer or smart inhaler, that device carries its own classification and performance obligations.
Sponsor	Holds ultimate GCP accountability for the reliability of trial data, even where execution is delegated.
eCOA / ePRO vendor	Where the app hosts assessments or recruits sensors, you may be operating a measurement instrument or MDSW — a different position from a passive host.
Logistics / provisioning vendor	Provisioning and the sourcing route shape where importer or distributor duties fall (MDR Arts 13, 14, 16); kitting can bring the assembler within Article 22 (systems and procedure packs).
Connectivity provider (eSIM / data plan)	Where traffic routes is set here — a security-in-transit and data-localization question that becomes a cross-border-transfer obligation only where a third-country party receives or accesses the data.
MDM / device-management vendor	The platform enforcing the locked-down state is itself part of what must be trusted; in qointa's assessment, constraining the device for a medical purpose can draw the vendor within MDR Article 16.
OS / firmware vendor	Updates can change validated behavior mid-study, moving the device across a perimeter with no protocol decision behind it.
Clinical systems vendors (EDC, RTSM, CTMS, eTMF)	The integration boundary is in validation scope; data provenance, timestamps and audit trail must survive the handoff.
CRO / sites	You operate the system under GCP, so where the device sits on the scale bears directly on how data capture is run and documented.
Participant	When their own phone is in the path (BYOD) — as instrument or as relay — their device, settings and behavior become part of the measurement.
IRB / Ethics Committee	Can require evidence of device suitability or device-side data integrity as a condition of its opinion (21 CFR Part 56; CTR 536/2014); in qointa's experience that evidence then forms part of the approved study record.
Regulators / inspectors	Examine the evidence for the device layer — FDA in the durable repository rather than on individual DHTs (Part 11 Q&A, Q23), EU inspectors against the EMA guideline's device-side controls; the control you can show at first inspection becomes the de facto baseline.

Inside the sponsor — “the sponsor” is not a single desk. The assessment is owned jointly across QA / GCP compliance, Regulatory Affairs, computerized-system validation and the study's project management.

Stakeholder responsibility matrix: the sponsor is accountable, every party assesses its own footprint

Stakeholder	Typically owns	RIA responsibility	Typical load
Sponsor	Overall trial conduct and vendor oversight	Accountable for the RIA being performed and for the reliability of trial data (E6(R3) s.3.6).	High
eCOA / ePRO vendor	The app and data capture	Assess whether the app is a measurement instrument or MDSW.	High
Phone manufacturer / OEM	Hardware and change notifications	Supply the specification and change data others' assessments rely on.	Med
Connected-device manufacturer	The wearable or biosensor	Carry the device classification and performance evidence.	High
Logistics / provisioning vendor	Provisioning, kitting and sourcing	Check for economic-operator duties (MDR Arts 13, 14, 16) and Article 22 systems / procedure packs.	Med
Connectivity provider (eSIM / data plan)	Connectivity and routing	Assess security in transit, data localization and any third-country access.	Med
MDM / device-management vendor	Locked-down configuration	Assess configuration-control implications and whether constraining the device draws MDR duties.	Med
CRO / sites	Local conduct and source data	Operate within the controls the RIA defines; surface changes.	Low

Typical load is indicative only — the actual depth for any party follows that deployment's role and triggers.

13. How qointa can help

qointa supports sponsors, vendors and CROs in turning the principle above into a **documented, proportionate decision** — and in keeping it current as a study evolves. Each service maps to a concrete deliverable.

Service	What you receive
RIA scoping & execution	A completed RIA for the specific study setup, scaled to the role and triggers in play — delivered on a reusable qointa RIA template.
Per-stakeholder mapping	A responsibility matrix identifying which party carries which obligation, so no duty is inherited unknowingly.
Framework gap analysis	A single-pass check of the deployment against MDR, IVDR, the AI Act, GCP and data-integrity expectations, with gaps flagged.
Lifecycle support	A baseline assessment plus a Trigger Register — the controlled record of software, firmware, vendor, route and country changes that reopen the RIA (QPP-08 — Trigger Register).
Audit & inspection readiness	A documented rationale pack that turns a defensible conclusion into evidence ready for inspection.

Practical next steps

1. Identify every device and system the trial relies on in a non-investigational capacity.
2. Place each on the role scale (Section 6) and run the triggers (Section 7).
3. Record the controls decision and its rationale, and assign the owning stakeholder.
4. Enter the material-change triggers in a Trigger Register, and revisit the assessment at each one.

Contact qointa for tailored RIA support

To scope an RIA for a specific study, or to review an existing deployment, get in touch with the qointa team: info@qointa.com

Scope and status

This paper sets out a regulatory position to inform a controls decision. It is not legal advice and does not itself determine device classification in any jurisdiction. The principle — **assess rather than assume** — applies wherever a trial runs, but the specific frameworks cited here are centered on the EU, US and ICH GCP environment; obligations in other jurisdictions may differ and should be confirmed locally; the UK position (MHRA) is addressed in QPP-06 — Inspection-Readiness and QPP-23 — Global Reconciliation. Final qualification and classification should be confirmed with qualified regulatory counsel and, where relevant, the applicable competent authority or notified body. Framework references reflect documents current at the date of issue.