Qity

A BRIEFING FOR MEDICAL DEVICE MANUFACTURERS

The gray areas between the Cyber Resilience Act and your medical device

Products to which the MDR or IVDR applies are excluded from the CRA under Article 2(2), and the exclusion attaches to the product rather than to the company. Issue is, many real portfolios are not that clean. A companion app that is free of charge, a gateway that ships with the device and is also sold on its own, an SDK offered to partners, a cloud service that delivers the medical function and is marketed separately as analytics, a research module, a wellness feature, a white-labeled build: each one sits in a zone where the answer depends on facts the marketing material rarely states. This briefing works through those gray areas, names the blind spots they create, and states what closes each one while covering scope, nine ecosystem cases, the reporting clock that starts on 11 September 2026, and the records that make a decision defensible.

A product, a connection, and everything the manufacturer keeps running behind it

The CRA applies to products with digital elements made available on the market in the course of a commercial activity, where the intended purpose or reasonably foreseeable use includes a direct or indirect data connection. Each element of that sentence is a place where a portfolio becomes unclear.

IN FORCE	FIRST OPERATIONAL DEADLINE	MAIN OBLIGATIONS
10 Dec 2024	**11 Sep 2026**	**11 Dec 2027**
Regulation (EU) 2024/2847 entered into force.	Article 14 reporting of actively exploited vulnerabilities and severe incidents begins.	Product, manufacturer and conformity obligations become generally applicable.

MADE AVAILABLE COMMERCIALLY

Software applications, operating systems, embedded software, connected hardware, network appliances, software components, mobile and desktop applications, certain cloud-dependent functionality and commercial open-source software all qualify as products with digital elements.

Blind spot. Free of charge does not mean outside commercial activity. Software supplied without a separate fee stays commercial where it supports a paid service, device, subscription or data offering.

CONNECTED, DIRECTLY OR INDIRECTLY

A connection may be physical or wireless, local or remote, mediated through another device, occasional, machine to machine, through an API, or through a gateway or cloud component. The product does not need to reach the public internet.

Blind spot. Software recorded as offline often is not. Installation, license verification, updates, synchronization and export each create relevant connectivity.

REMOTE DATA PROCESSING IS PART OF THE PRODUCT

Remote data processing forms part of the product where the manufacturer develops it or carries responsibility for it, and its absence would stop the product performing one of its functions. A manufacturer-controlled inference service, a backend authentication service or a remote configuration service integral to operation sits inside the boundary. A corporate website or a generic external cloud service outside the manufacturer's responsibility does not, although NIS2, the GDPR and contracts may still apply to it.

FIVE QUESTIONS THAT SETTLE THE BOUNDARY

1. Does the manufacturer develop it or carry responsibility for it?
2. Is it necessary for one or more product functions?
3. Is it supplied as part of the product offering?
4. Can the product perform those functions without it?
5. Is the function within the intended or foreseeable use?

ARTICLE 2(2), AND ITS LIMIT

The CRA does not apply to products with digital elements to which Regulation (EU) 2017/745 or 2017/746 applies. Risk class is irrelevant: Class I to Class III, IVDR Class A to Class D, software or hardware, connected or local. The exclusion reaches the product only. It does not reach the portfolio, the platform, the brand or the company.

COMPONENTS, IN BOTH DIRECTIONS

A component supplied separately can carry its own CRA obligations even when the device that incorporates it is excluded. The supplier declaration, support period, disclosure policy and SBOM are supplier evidence.

Blind spot. A supplier conformity claim does not transfer your MDR duty for integration, verification, known vulnerabilities and post-market monitoring, and it does not answer whether your product is affected.

> *"A shared codebase, shared brand, shared cloud environment or shared cybersecurity program does not make all modules subject to the same legislation."*

Nine products around one device, and what each one gets wrong

Each row is a marketed offering, not a repository or a brand. The position is a starting hypothesis. The third column names the assumption that fails in review and the record that closes it.

SCENARIO	LIKELY POSITION	THE BLIND SPOT, AND WHAT CLOSES IT
Standalone medical device software Diagnosis, monitoring, prediction, treatment support	MDR applies. CRA excluded under Article 2(2).	Teams read the exclusion as portfolio-wide. Record it per product, and keep MDR cybersecurity, lifecycle and PMS evidence current.
IVD software Information from in vitro examination of specimens	IVDR applies. CRA excluded.	Analytical modules sold to laboratories outside the IVDR purpose need their own qualification.
Companion app that controls the device Shows medical output or changes parameters	Part of the device, a device itself, or an accessory. Where MDR applies, CRA is excluded.	The label companion app decides nothing. Qualify on function, then bring the app, interfaces, backend and update path into the device risk file.
Companion app, non-medical functions only Account administration, education, support	Possibly not an MDR product or accessory. Assess the CRA on its own facts.	Free of charge and bundled in the same store listing do not remove commercial supply. Decide whether it is a separate product.
Cloud delivering the medical purpose Client sends data, cloud performs the analysis	Excluded where the cloud functionality forms part of the MDR or IVDR product and is necessary to deliver its intended medical purpose.	Controlling a service through the device QMS does not by itself establish the exclusion. Document the regulated product boundary; separately supplied infrastructure, analytics or platform functionality needs its own assessment.
General cloud platform, supplied separately Data management or analytics sold on its own	The independently marketed platform may be in CRA scope.	The same instance can be inside the device and a separate product. Split claims, documentation, support period and reporting route.
Deployment appliance or gateway Connectivity, remote access, data routing	Depends on whether it is part of the device, an accessory, or a general product.	Shipping with the device is not the test. Record whether it assists the medical function and whether it is also sold alone.
SDK or API for partners Offered commercially for general integration	May be a separately supplied product or component under the CRA.	Internal tooling opened to partners changes status quietly. Define versioning, support, disclosure and integration duties.
Update or distribution service Software that pushes updates to devices	Inside the device framework where integral. CRA may apply where sold as a general product.	Control update authenticity, integrity, rollback, release approval and deployment evidence on either route.

ONE CODEBASE, SEVERAL REGIMES

One platform can carry a regulated diagnostic module, a non-medical workflow module and an administrative dashboard. Each marketed configuration needs its own qualification. White labeling adds a further trap: a party that places a product under its own name becomes the manufacturer for CRA purposes.

SUBSTANTIAL MODIFICATION, LATER

A product on the market before 11 December 2027 can still be pulled in where it is substantially modified after that date and made available again: a new network-facing function, a changed trust architecture, a new intended purpose. A security update that reduces risk generally is not substantial. Document the assessment either way, because the labels patch and minor release decide nothing.

The clock starts at awareness, fifteen months before the rest of the CRA

Reporting applies before the main requirements do, so a manufacturer may still be building its technical documentation while already required to recognize and report qualifying events, including events affecting products already on the market.

ACTIVELY EXPLOITED VULNERABILITY

24 hours	Early warning from awareness.
72 hours	Vulnerability notification.
14 days	Final report, once a corrective or mitigating measure is available.

A theoretical vulnerability, a proof of concept or a vulnerability in a component is not automatically active exploitation. Assess whether your product is affected and whether reliable evidence of malicious exploitation exists.

SEVERE INCIDENT AFFECTING PRODUCT SECURITY

24 hours	Early warning from awareness.
72 hours	Incident notification.
One month	Final report, within one month of the 72-hour notification.

An incident is severe where it negatively affects, or is capable of negatively affecting, the product's ability to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions, or where it has led, or could lead, to malicious code being introduced or executed in the product or the user's networks and information systems. Scale, duration, affected markets and operational impact belong in the impact assessment, not in the threshold.

MINIMUM WORKFLOW

01 **Intake** Receive the vulnerability or incident report.	02 **Preserve** Logs, evidence, versions, affected configurations.	03 **Identify product** Exact product, version, market, legal regime.	04 **Assess CRA scope** In scope, or excluded under Article 2(2).
05 **Qualify event** Active exploitation or severe incident criteria.	06 **Escalate** Notify the incident and regulatory team at once.	07 **Early warning** Submit available information within 24 hours.	08 **Investigate** Root cause, impact and exposure analysis.
09 **72-hour notification** Provide the fuller required notification.	10 **Correct and communicate** Deploy validated mitigation. Inform impacted users, and where appropriate all users, of the measures they can take.	11 **Final report** 14 days for a vulnerability, one month for an incident.	12 **Close and improve** CAPA, risk update, documentation, effectiveness review.

THREE BLIND SPOTS ON THE CLOCK

Awareness is undefined until you define it. State which personnel create organizational awareness, how reports arrive, how service providers escalate, and who covers weekends. A process that waits for technical certainty misses 24 hours.

Excluded product, in-scope neighbor. An event can start in an excluded device and land in a gateway, SDK or platform that is not. Triage by affected product and version, not by team.

One event, several clocks. Triggers and deadlines differ, so assess every route rather than reusing the first conclusion.

THE ROUTES TO ASSESS

CRA	Actively exploited vulnerabilities and severe product security incidents, through the Single Reporting Platform, CSIRTs and ENISA.
MDR / IVDR	Serious incidents, field safety corrective actions, trend reporting.
GDPR	Personal data breaches presenting risk to natural persons.
NIS2	Significant incidents for covered entities, on its own clocks.
Contracts	Customer, insurer, supplier and partner notification duties.

Use one internal event identifier across all assessments and keep the rationale for each route separate. A CRA severe incident may sit below the MDR health-harm threshold, and an MDR serious incident may involve no exploitation.

Eight assumptions that create blind spots, and the register that removes them

CLAIMS THAT DO NOT SURVIVE REVIEW

"We are a medical device manufacturer, so the CRA does not apply to us."

The exclusion attaches to MDR and IVDR products, not to the company or the portfolio.

"Our product is CE marked, so the CRA is covered."

One CE mark, supported by a declaration that identifies each applicable act. Conformity is assessed per act.

"We hold ISO/IEC 27001, so the product is CRA compliant."

Organizational certification does not replace product-specific CRA evidence.

"It was sold before December 2027, so no CRA obligation applies."

Article 14 reporting applies from September 2026, and substantial modification can trigger more.

"The software runs in a hospital, so it is excluded."

Administrative and general-purpose software used in healthcare can remain in CRA scope.

"Every connected medical device must comply with both regimes."

The CRA excludes MDR and IVDR products. Cybersecurity duties remain under the MDR.

"The CRA requires publication of the full SBOM."

It requires machine-readable component and vulnerability documentation, covering at least top-level dependencies.

"The MDR revision has removed the exemption."

The December 2025 proposal would add an MDR and IVDR route for reporting actively exploited vulnerabilities and severe incidents through Eudamed. It does not remove the Article 2(2) exclusion, and as at 5 August 2026 the procedure is ongoing.

REGULATORY APPLICABILITY REGISTER

One controlled record per digital product, module and component, with the rationale written down rather than assumed:

- Product and version
- Intended purpose
- Claims and labeling
- Market status
- Economic operator role
- Annex III or IV category
- Standards relied upon
- Support period
- Approval
- MDR / IVDR qualification
- Accessory status
- CRA status and rationale
- Other applicable legislation
- CRA product category
- Conformity assessment route
- Notified body needed
- Reporting contacts
- Review triggers

Category decides the route. Most products use internal control. Important Class I products may use it only where harmonized standards, common specifications or a certification scheme are fully applied, and important Class II and critical products take third-party routes. A gateway, network-management component, firewall or operating system often lands in these categories, so record the Annex III or IV rationale against the technical descriptions in Implementing Regulation (EU) 2025/2392. CRA classes are unrelated to MDR classes.

Support period. At least five years unless the product is reasonably expected to be in use for less time, with the end date clear at the time of purchase. Issued security updates stay available for at least ten years, or the remainder of the support period where that is longer.

WHAT THE QMS HAS TO CONNECT

SBOM governance Linked to product version, release record, suppliers, vulnerabilities and change control.	**Vulnerability management** Intake, severity, applicability, exploitability, remediation target, disclosure, closure.
Supplier control Capability, disclosure policy, update commitments, support period, escalation.	**Change and release** MDR change significance and CRA substantial modification on one record.
Post-market intake One triage that routes complaints, incidents and vulnerabilities to the right regime.	**Training and review** The 24-hour escalation trained, and readiness reviewed by management.

> *"A medical device QMS is a strong operational foundation, and it still has to be extended to cover CRA product classification, support periods, SBOMs, vulnerability reporting and declarations for independently in-scope products."*

Seven questions about one connected product you supply today

Answer for a single marketed product rather than for the company. More than two answers of no indicates a position that is asserted rather than documented, which is where the gray areas become findings.

Scope	Is there a documented applicability decision for every marketed module and configuration, and not only for the regulated device?	Yes / Partly / No
Boundary	Does the technical documentation state which remote services sit inside the product boundary and which sit outside it?	Yes / Partly / No
Art. 14	Can a report received on a Saturday reach the accountable owner and produce an early warning within 24 hours?	Yes / Partly / No
Criteria	Are written criteria in place for active exploitation and for a severe incident, applied by a named function?	Yes / Partly / No
SBOM	For each released version of an in-scope product, is there a machine-readable SBOM linked to vulnerability intelligence?	Yes / Partly / No
Support	Is a support period of at least five years declared, or a shorter period justified by an expected use time of less than five years, and is it consistent with the service life of the associated medical system?	Yes / Partly / No
Category	Is the CRA product category recorded for each in-scope product, with the conformity route and any notified-body involvement that follows from it?	Yes / Partly / No

SEQUENCE

Before 11 Sep 2026	Next 90 days	2026 to 2027	Before 11 Dec 2027
Accountable owner, product inventory, exclusions product by product, severity criteria, 24-hour escalation, platform access, tabletop exercise, out-of-hours cover.	First applicability register, documented product boundaries, risk-assessment templates, SBOM generation, support periods, conformity routes, documentation gaps.	Product-level risk assessments, missing essential controls, secure-by-default validation, supplier evidence, support declarations, user security information, notified body where required.	Conformity assessment per in-scope product, approved technical documentation, EU declaration of conformity, CE-marking evidence, release gates that cannot be bypassed.

ASSESS APPLICABILITY

qity.app

Map products, modules, configurations and dependencies against the CRA, the MDR and the IVDR, and produce a documented position for each product.

Start the assessment

OPERATIONALIZE IT IN THE QMS

qity.be

Hold classifications, risks, design controls, suppliers, software components, SBOMs, vulnerabilities, incidents, changes, CAPAs and post-market evidence as controlled records inside Jira and Confluence.

See the Qity QMS

Summary and interpretation only, current as at 5 August 2026, and not legal advice. Applicability is decided for each product, module and economic operator role on the applicable legislation and the intended purpose. Sources: Regulation (EU) 2024/2847, Regulations (EU) 2017/745 and 2017/746, the Commission practical CRA guidance of 27 July 2026, Implementing Regulation (EU) 2025/2392, MDCG 2019-16 rev.1 and COM(2025) 1023. Qity supports structured CRA applicability, implementation and evidence management. The manufacturer retains responsibility for conformity.