European Journal of Risk Regulation (2026), 1–20
doi:10.1017/err.2026.10167

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

A Transfer Route Without a Stop Route: Safety Execution Under the Proposed Article 5(5) Amendments to the MDR and IVDR

Andreas Peters

Rosenheim Technical University of Applied Sciences, Germany
Email: a.peters81@icloud.com

Abstract

COM (2025) 1023 would permit specified transfers of in-house devices between health institutions, coupled with bilateral traceability and recipient-to-transferor incident reporting, yet it does not state how a safety finding becomes a release-specific instruction, reaches every deployment, produces local cessation of use and returns as verified closure. This article examines that missing execution link. Union safety law mandates identification and then treats it as a proxy for actionability, although traceability and a use-stop ask different questions and need different record units; the argument is developed against ordinary recall rules and tested on software, assay, printed-device, emergency and onward-transfer cases. A two-institution record should connect controlled release identity, local acceptance and deployment, change history, incident escalation, scoped use-stop, execution acknowledgement, remediation and custody closure. The operative communication and acknowledgement duties belong in Article 5(5) itself, with modality-dependent fields left to guidance. So designed, the exemption keeps its exceptional character without treating the market-route recall framework as directly applicable.

Keywords: Article 5(5) MDR/IVDR; in-house medical devices; safety corrections

I. Introduction: the instruction that did not stop use

Assume that a university hospital writes and validates software selecting an assay pathway. A second hospital receives it under the proposed Article 5(5) route. Months later, the originator finds that one build can suppress a clinically significant warning and sends an urgent message. The recipient says that its laboratory modified the interface and may run an earlier build. Neither institution can establish which build is active, whether satellite access was disabled, or whether the application moved onward. The message exists. Cessation of use does not follow.

The example is hypothetical. Its legal difficulty is not. Regulation (EU) 2017/745 (MDR) and Regulation (EU) 2017/746 (IVDR) presently allow a health institution to manufacture and use a device under Article 5(5), subject to the conditions stated there, only while the device is not transferred to another legal entity.[1] COM (2025) 1023 would relax that

[1] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L117/1 (MDR), Art. 5(5)(a); Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing

© The Author(s), 2026. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/err.2026.10167

boundary for specified transfers between health institutions. The proposed language requires traceability at both institutions and directs the receiving institution to report a device-related incident to the transferring institution.[2] At the time of writing, the measure remained a proposal in procedure 2025/0404(COD). No present transfer can rely on it.

Movement and backward reporting those additions permit; what they leave undefined is the affected release, the issuer, recipient execution, returned evidence and closure. Effective corrective action still requires a precise forward instruction to reach every deployment and an acknowledgement to return. Without those links, "traceability" may describe a record without making the device addressable for safety action.

Three strands of scholarship approach this gap without closing it. Work on device qualification and responsibility asks whether a given artefact is a regulated device, and who answers once a patient has been harmed; it addresses attribution after the event rather than the mechanics of a correction.[3] Research on identification and traceability, including the unique-device-identifier literature and studies of version identity in medical software, establishes how an object may be named, but a name is not yet an instruction. Enforcement scholarship in Union product safety asks whether competent authorities have a legal basis to organise a recall across overlapping regimes, and answers it for market actors inside market machinery.[4] None of the three addresses a corrective command that must cross a legal-entity boundary between two institutions which are, by the very terms of the exemption, not market operators at all.

The question here is accordingly narrow and, in its narrowness, general: if the transfer exception becomes law, what minimum legal and record structure lets a safety decision taken in one health institution produce a verified change in the state of use in another? Three sub-questions follow. What must be identified before an instruction can be scoped? Who may command, who must execute, and what follows when either is silent? What evidence closes the event? A closed-loop use-stop chain supplies the connecting structure; "use-stop" is functional, not statutory, language.

Two claims give the enquiry its wider interest. The first is conceptual. Union safety law routinely mandates identification and then treats it as a proxy for actionability, although the two answer different questions: traceability is retrospective and evidentiary, asking where an object went, whereas a use-stop is prospective and operational, asking which

Directive 98/79/EC and Commission Decision 2010/227/EU [2017] OJ L117/176 (IVDR), Art. 5(5)(a). The consolidated MDR text used for this article is dated 1 January 2026; the consolidated IVDR text is dated 10 January 2025.

[2] European Commission, "Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2017/745, (EU) 2017/746, (EU) 2022/123 and (EU) 2024/1689 as regards simplifying and reducing the burden of the rules on medical devices and *in vitro* diagnostic medical devices" COM (2025) 1023 final, Arts 1(5) and 2(5).

[3] M. Prictor, "Where Does Responsibility Lie? Analysing Legal and Regulatory Responses to Flawed Clinical Decision Support Systems When Patients Suffer Harm" (2023) 31 Medical Law Review 1, 5, doi: 10.1093/medlaw/fwac022; T. Minssen, M. Mimler and V. Mak, "When Does Stand-Alone Software Qualify as a Medical Device in the European Union? The CJEU's Decision in SNITEM and What It Implies for the Next Generation of Medical Devices" (2020) 28 Medical Law Review 615, doi: 10.1093/medlaw/fwaa012; B Solaiman and A Malik, "Regulating Algorithmic Care in the European Union: Evolving Doctor–Patient Models through the Artificial Intelligence Act (AI-Act) and the Liability Directives" (2025) 33 Medical Law Review fwae033, doi: 10.1093/medlaw/fwae033; M. Quigley and S. Ayihongbe, "Everyday Cyborgs: On Integrated Persons and Integrated Goods" (2018) 26 Medical Law Review 276, doi: 10.1093/medlaw/fwy003; A. M. McMahon and O. I. Kolawole, "Intellectual Property Rights over 'Integrated' Medical Devices: The Potential Health Impacts and Bioethical Implications of Rightsholders' Control" (2025) 33 Medical Law Review fwaf001, doi: 10.1093/medlaw/fwaf001.

[4] B. L. Tennant and others, "Communicating Medical Device Recalls: A Rapid Review of the Literature" (2024) 123 Patient Education and Counseling 108244, doi: 10.1016/j.pec.2024.108244; T. I. Morgenthaler and others, "Rapid Response to Medical Device Recalls: An Organized Patient-Centered Team Effort" (2022) 18 Journal of Clinical Sleep Medicine 663, doi: 10.5664/jcsm.9748.

https://doi.org/10.1017/err.2026.10167

release sits at which deployment, in what state, and on whose evidence that state has changed. Record units that satisfy the first requirement need not satisfy the second, and a regime legislating the one while assuming the other produces instruments that identify without commanding. The second claim concerns method. Article 5(5) looks like a niche, and that is precisely its analytical value: because the exemption disapplies most of the Regulations, the market apparatus of economic operators, notified bodies, field-safety machinery and central databases is absent, leaving the underlying requirement exposed. What other regimes answer by institutional layering, the exempt route must answer from first principles. The design proposed below is addressed to the medical-device file, but the gap it names recurs wherever a corrective command must reach a non-market actor across an organisational boundary.[5]

Seeking a model for such a command, one turns first to ordinary recall law, which supplies a comparator rather than a ready-made answer. Recall, field safety corrective action and field safety notice belong to a manufacturer- and market-linked scheme, whereas Article 5(5) disapplies most of the Regulations while retaining Annex I and its stated conditions; a qualifying transfer remains governed by that express derogation. Whether a particular supply also falls within Article 2's market definitions depends on its facts and is not decided here, and Chapter VII cannot be made binding merely by analogy. The market route serves only to test what an executable response contains.

That distinction has an immediate consequence: public notification identity need not identify the release running at the recipient. Bianchini and colleagues identify the traceability difficulties posed by evolving medical software.[6] Article 5(5) need not reproduce commercial UDI. It needs an object precise enough for corrective action across two institutions.

What this article contributes is accordingly event-specific: an account of the safety decision taken after the object and its clinical control have separated. Under the proposed wording an incident can be reported backwards. Unresolved is whether an identified safety instruction can move forwards, be executed locally and return as verified closure. Figure 1 is a schematic prepared for this article. It maps that discontinuity at the legal-entity boundary: the backward incident-reporting and bilateral traceability links reflect the Commission proposal, while the forward safety-instruction and closure links are this article's recommendations.

II. A transfer route without a recall route

1. Existing law keeps manufacture and use inside one legal person

Article 5(5) is an exemption with a retained safety core, not a regulatory absence. Under the MDR, a device manufactured and used within a Union health institution is treated as having been put into service. Most requirements of the Regulation then fall away only if the applicable Annex I requirements and every condition in Article 5(5) are satisfied. The IVDR follows the same structure, with additional provisions concerning medical-laboratory

[5] Commission Decision (EU) 2025/2371 of 26 November 2025 declared functional the Eudamed electronic systems on registration of economic operators, the UDI database and device registration, notified bodies and certificates, and market surveillance; their use became mandatory on 28 May 2026, while the vigilance and clinical-investigation modules await a corresponding declaration. Each system addresses market actors, and a device manufactured and used under Article 5(5) is registered in none of them.

[6] E. Bianchini and others, "Unique Device Identification and Traceability for Medical Software: A Major Challenge for Manufacturers in an Ever-Evolving Marketplace" (2019) 93 Journal of Biomedical Science 103150, doi: 10.1016/j.jbi.2019.103150.

https://doi.org/10.1017/err.2026.10167

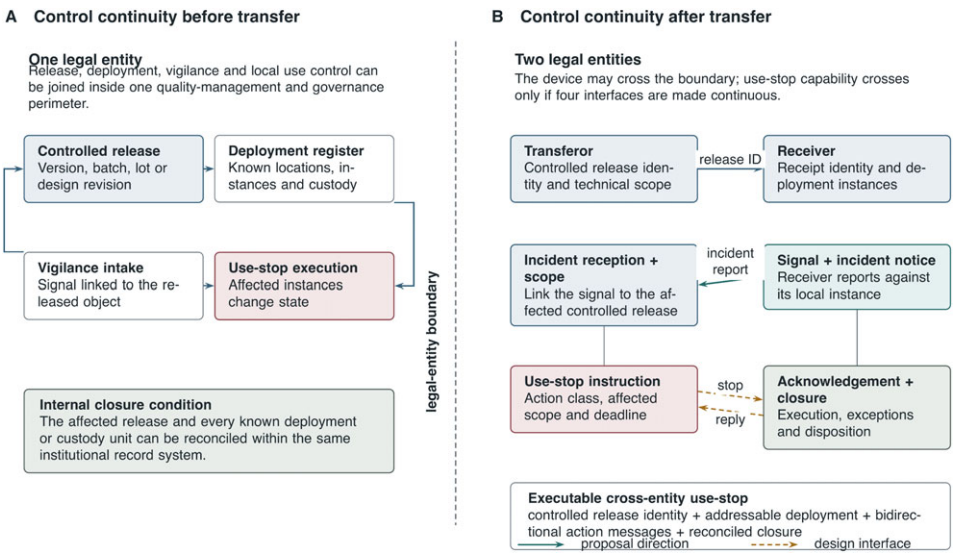


Figure 1. Control continuity at a legal-entity transfer. Within one institution, controlled release, deployment, vigilance and local use control can remain joined. Transfer separates release identity from the receiver's deployments. Bilateral traceability and receiver-to-transferor incident information are stated in the Commission proposal; the remaining links are author recommendations.

Alt text: Two panels compare joined control inside one legal entity with a transferred device. The second adds release identification, backward incident reporting, a forward use-stop instruction, reply and reconciled closure.

competence and the documentation of class D devices.[7] The present point (a) is categorical: the device may not be transferred to another legal entity. Point (b) places manufacture and use under appropriate quality-management systems. Public identification, authority access, technical documentation, manufacture in accordance with that documentation, review of clinical experience and necessary corrective action complete the parts relevant here.[8]

That arrangement matters for a reason easily missed when Article 5(5) is read as a checklist. The rule does not have to design a message path between independent institutions because its boundary condition prevents that separation. A hospital may divide technical, clinical and governance work among departments, sites and laboratories, yet the legal person remains able to prescribe internal authority and escalation through one institutional system. Whether a particular network is one legal person is a factual and national-law question; a shared brand, common procurement system or regional label does not answer it. MDCG 2023-1 therefore treats manufacture and use within the same health institution as a condition of the current exemption and advises institutions to examine the legal-entity boundary.[9]

[7] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices [2017] OJ L117/1 (MDR), Arts 5(4)–(5); Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices [2017] OJ L117/176 (IVDR), Arts 5(4)–(5). Consolidated texts: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02017R0745-20260101> and <https://eur-lex.europa.eu/eli/reg/2017/746/2025-01-10> (last accessed 14 July 2026).

[8] MDR Art. 5(5)(a)–(h); IVDR Art. 5(5)(a)–(i). The IVDR documentation duty in Art. 5(5)(g) applies to class D devices unless a Member State extends it, while Art. 5(5)(h) supplies the corresponding production–documentation connection.

[9] Medical Device Coordination Group, "Guidance on the health institution exemption under Article 5(5) of Regulation (EU) 2017/745 and Regulation (EU) 2017/746" (MDCG 2023-1, January 2023) 5–7, 13–14 <https://health.ec.europa.eu/system/files/2023-01/mdcg_2023-1_en.pdf> (last accessed 14 July 2026). MDCG guidance is not legally binding: European Commission, "Guidance – MDCG endorsed documents and other guidance" <https://

https://doi.org/10.1017/err.2026.10167

Within that single-person arrangement, the binding safety logic is continuous rather than episodic. Annex I describes risk management as an iterative process throughout the device lifecycle, with systematic updating. Software must be developed and manufactured with attention to its development lifecycle, risk management, information security, verification and validation. IVD performance remains tied to intended purpose, and devices used with other products must retain safe compatibility and interoperability.[10] Article 5(5)'s direction to review experience and take necessary corrective action sits within that retained Annex I setting. MDCG 2023-1 reads device identification as capable of forming part of a tracking system for affected products and patients; it also places lifecycle risk management, monitoring and corrective action within an appropriate in-house QMS. Kahles and colleagues describe one pathology service's implementation of device-specific IVDR Annex I requirements. Straathof and colleagues report an MDR Article 5(5) development case in which applicable Annex I requirements were checked through risk analysis and verification of a patient-tailored brachytherapy applicator and associated software. In an EFLM joint opinion, Vanstapel and colleagues argue that ISO 15189 can be a sufficient instrument for compliant in-house manufacture; MDCG 2023-1 cautions that ISO 15189 alone does not establish an appropriate QMS covering all manufacturing and relevant Annex I requirements.[11] These accounts do not yet allocate safety tasks across two legal persons.

Below the Union text, national implementation shows how much operational content may exist. Portugal, for example, requires a notified in-house MDR device to sit within a QMS covering design, manufacture, control, release, internal distribution, use and traceability, and requires a system for recording and analysing clinical-use experience.[12] Release and internal distribution can thus be stated expressly, but no Union-wide recipient duty follows from one national rule.

2. *The proposed text opens the boundary but stops at information exchange*

COM (2025) 1023 would replace the present prohibition with a qualified permission. A device could be transferred to another health institution where the move is duly justified by public health, patient safety or patient health, or where it prepares for or responds to a public-health emergency. In both regimes, transferor and recipient would have to maintain device traceability, and the recipient would report any incident related to the device back to the transferor.[13] All of this remains proposed text. Procedure 2025/0404(COD) remains ongoing; a Council progress report dated 5 June 2026 records

health.ec.europa.eu/medical-devices-sector/new-regulations/guidance-mdcg-endorsed-documents-and-other-guidance_en> (last accessed 14 July 2026).

[10] MDR annex I paras 3, 14.5 and 17.1–17.4; IVDR annex I paras 3, 9.1, 13.5 and 16.1–16.4.

[11] MDCG 2023-1 supra, note 9 9–12. See also A. Kahles and others, "Regulation (EU) 2017/746 (IVDR): Practical Implementation of Annex I in Pathology" (2023) 44 (Suppl 2) Pathologie 86, doi: 10.1007/s00292-023-01274-6; R. Straathof and others, "Patient-Tailored Brachytherapy Applicator Development in Compliance with the EU Medical Device Regulation" (2026) 145 Physica Medica 105783, doi: 10.1016/j.ejmp.2026.105783; F J. L. A. Vanstapel and others, "ISO 15189 Is a Sufficient Instrument to Guarantee High-Quality Manufacture of Laboratory Developed Tests for In-House-Use Conform Requirements of the European *In-Vitro*-Diagnostics Regulation: Joint Opinion of Task Force on European Regulatory Affairs and Working Group Accreditation and ISO/CEN Standards of the European Federation of Clinical Chemistry and Laboratory Medicine" (2023) 61 Clinical Chemistry and Laboratory Medicine 608, doi: 10.1515/cclm-2023-0045.

[12] Decreto-Lei n.º 29/2024, de 5 de abril (Portugal), Arts 6(2)(a)(iii)–(vii) and 7 <https://diariodarepublica.pt/dr/detalhe/decreto-lei/29-2024-859517101> (last accessed 14 July 2026).

[13] COM (2025) 1023 *supra*, note 2, Arts 1(5)(a) and 2(5)(a) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC1023> (last accessed 14 July 2026).

https://doi.org/10.1017/err.2026.10167

continuing article-by-article examination and the need for further work on several parts of the package.[14]

Two textual changes sharpen the enquiry. For the MDR, the Commission proposes a new documentation formulation and deletion of point (g), which obliges the institution to ensure manufacture according to the point (f) documentation; for the IVDR it narrows the documentation arrangement and deletes the counterpart point (h). Remaining Annex I, QMS and corrective-action duties should prevent an exaggerated reading of these deletions. Even so, the express sentence tying the manufactured instance to its documentary baseline would disappear just as the law begins to tolerate movement to a separate user institution. Traceability is added, but its unit is left unstated: family, design revision, software build, reagent lot and individual printed article can each be "the device," and only some levels let a later safety instruction reach the affected object.

Alongside those textual changes, the surrounding eligibility conditions would also shift asymmetrically. The MDR would retain point (c), coupled with a maximum ten-year continuation after a market device can meet the target group's needs; the IVDR would delete its present equivalent-device condition in point (d). The IVDR proposal would also extend Article 5(5) to specified clinical-research laboratories.[15] Those broader changes are not evaluated here; the analysis assumes that a particular transfer satisfies every threshold condition in the final regime.

Presenting the reform as simplification, the Commission's evaluation does not specify a recipient-side use-stop procedure for an Article 5(5) transfer. In the related debate, Cobbaert and colleagues, writing for the EFLM, favour more flexible in-house IVD arrangements while retaining essential safety and performance safeguards.[16] The proposal states a justified transfer, traceability at both institutions and an incident message back, but not the intervening control states or the closing event.

A defined-term question nevertheless remains. "Incident" in Article 2 is framed by reference to a device made available on the market. Some qualifying transfers may themselves satisfy "making available," which extends to supply in the course of a commercial activity whether for payment or free; others may not.[17] The proposal does not specify whether its Article 5(5) duty uses incident only within that Article 2 scope or as a route-specific trigger. The central conclusion does not depend on the answer: even a valid backward incident report is not a forward instruction, local execution duty or closure record.

3. *Recall is the comparator, not the governing classification*

Ordinary recall law provides a demanding comparison. The MDR defines recall as a measure aimed at obtaining the return of a device already made available to an end

[14] EUR-Lex, "Procedure 2025/0404/COD" (status: Ongoing) <https://eur-lex.europa.eu/procedure/EN/2025_404> (last accessed 14 July 2026); Council of the European Union, "Regulation to simplify rules on medical and in vitro diagnostic devices – Progress report" ST 9801/26 (5 June 2026) paras 8–19 <https://data.consilium.europa.eu/doc/document/ST-9801-2026-INIT/en/pdf> (last accessed 14 July 2026).

[15] COM (2025) 1023 supra, note 2 Arts 1(5)(a)(i)–(iii) and 2(5)(a)(i)–(iii), including the MDR documentation change and deletion of point (g), and the IVDR documentation change and deletion of point (h).

[16] European Commission, "Evaluation on the Targeted evaluation of Regulation (EU) 2017/745 on Medical Devices and Regulation (EU) 2017/746 on In Vitro Diagnostic Medical Devices" (Commission Staff Working Document) SWD (2025) 1051 final <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52025SC1051> (last accessed 14 July 2026). See also C Cobbaert and others, "EFLM Position Statement on the Proposed 2025/0404(COD) IVDR Amendment of Article 5.5" (2026) 64 Clinical Chemistry and Laboratory Medicine 1455, doi: 10.1515/cclm-2026-0580.

[17] MDR Arts 2(27) and 2(64); IVDR Arts 2(20) and 2(67); COM (2025) 1023 supra, note 2 Arts 1(5)(a)(iii) and 2(5)(a)(iii).

https://doi.org/10.1017/err.2026.10167

user; the IVDR uses the same structure. A field safety corrective action is action by a manufacturer, for technical or medical reasons, to prevent or reduce serious-incident risk associated with a device made available on the market.[18] Chapter VII then connects manufacturer investigation, competent-authority assessment, a field safety notice, correct device identification and instructions to users. MDR Article 89(8) and IVDR Article 84(8) require the notice to identify the device, explain the risk and state the user action.[19]

None of this may simply be declared applicable to the exempt route. Article 5(5) disapplies the Regulation apart from the relevant Annex I requirements once its conditions are met. The defined market event, the economic-operator structure and the manufacturer-centred vigilance procedure therefore cannot be imported wholesale merely because a hospital needs to retrieve or correct a device. MDCG 2023-3 Rev.2 illustrates why the comparison remains valuable: its non-exhaustive FSCA examples include return, exchange, modification, destruction, changed maintenance or calibration advice, training, software update or rollback, patient or sample retesting and review of earlier results.[20] These examples demonstrate that a safety correction is not synonymous with physical return. They remain market-route guidance.

That negative boundary finds confirmation in the Commission's 2025 post-market-surveillance guidance. MDCG 2025-10 expressly excludes the Article 5(5) health-institution requirements from its scope, although it recalls that institutions are expected to review in-house use experience and take necessary corrective action.[21] A transferred in-house device therefore needs a functional counterpart to recall: one able to stop use and account for the affected object without converting the transfer into an ordinary placing-on-the-market event by analogy.

Read in context, the new incident sentence does more than exchange data: its express cross-reference to point (h) or (i) supports an inference that the transfer side must use the report in experience review and corrective action. That is the strongest textual answer to this article, and it remains incomplete. Point (h) or (i) names "the health institution"; traceability does not say which institution decides, which must implement, or what follows from silence. A QMS or transfer agreement can implement those duties but cannot settle the statutory trigger, competent-authority allocation or an unrecorded downstream recipient's obligations. Table 1 separates the stated elements from the unresolved execution points.

This article assumes that both entities meet the applicable health-institution definition, manufacture remains non-industrial and every amended Article 5(5) threshold is satisfied. A non-qualifying supply may instead engage the ordinary market regime; its classification under Article 2 is outside the enquiry. Legislative developments are stated as at 26 July 2026; online sources were otherwise last accessed on 14 July 2026. The file remains open in the ordinary legislative procedure.

[18] MDR Art. 2(62), (68) and (69); IVDR Art. 2(65), (71) and (72).

[19] MDR Art. 89(1)–(10), especially Art. 89(8); IVDR Art. 84(1)–(10), especially Art. 84(8). See also Commission Notice, "The Blue Guide on the implementation of EU product rules 2022" (2022/C 247/01) [2022] OJ C247/1, sections 2.2–2.4, for the general market concepts.

[20] Medical Device Coordination Group, "Questions and Answers on vigilance terms and concepts as outlined in Regulation (EU) 2017/745 and Regulation (EU) 2017/746" (MDCG 2023-3 Rev.2, January 2025) question 17, 20–22 <https://health.ec.europa.eu/document/download/af1433fd-ed64-4c53-abc7-612a7f16f976_en?filename=mdcg_2023-3_en.pdf> (last accessed 14 July 2026).

[21] Medical Device Coordination Group, "Guidance on post-market surveillance of medical devices and *in vitro* diagnostic medical devices" (MDCG 2025-10, December 2025) 4 <https://health.ec.europa.eu/document/download/a9ad86b7-1b8e-4bae-beb4-48b2b3ed2f05_en?filename=mdcg_2025-10_en.pdf> (last accessed 14 July 2026).

https://doi.org/10.1017/err.2026.10167

Table 1. Textual basis and unresolved execution point.

Element	Legal basis	What the text establishes	What the text does not establish
Annex I safety baseline	Current MDR and IVDR Art. 5(5)	Applicable general safety and performance requirements remain binding for a qualifying in-house device	No named cross-entity command and acknowledgment route
Appropriate quality management	Current Art. 5(5)(b)	Manufacture and use occur under appropriate quality-management systems	No stated interface between the systems of two legal entities
Experience review and corrective action	MDR Art. 5(5)(h); IVDR Art. 5(5)(i)	The health institution reviews clinical-use experience and takes necessary corrective action	No actor allocation after transfer, response deadline or closure condition
Limited transfer ground	Proposed replacement of point (a)	A transfer to another health institution may preserve the exemption where the stated ground is met	No present transfer entitlement, general authorisation procedure or onward-transfer rule
Bilateral traceability	Proposed new sentence in Art. 5(5)	Transferor and recipient maintain traceability of the device	No prescribed grain for family, release, lot, instance, endpoint or deployment
Incident information	Proposed new sentence in Art. 5(5)	The recipient reports a device-related incident to the transferor	No timing, required content, confirmation, forward safety instruction, non-response rule or completed-action evidence
Production–documentation link	Current MDR Art. 5(5)(g) and IVDR Art. 5(5)(h); proposed deletion	Present law expressly links manufacture with the relevant documentation	The proposal does not state how release drift is controlled after the sentence is removed
Public device identity	Current Art. 5(5) declaration duties and national practice	A public administrative object may be named or described	Public identity does not by itself identify the transferred release, local deployment or post-action state

III. From traceability to an executed use-stop

1. The object must be fixed at release

Traceability answers a question only after its object has been selected. A record stating that "the assay" travelled from institution A to institution B supports administrative history while remaining useless for a correction affecting reagent lot R17 on instrument configuration C3; the same defect appears where "the software" covers three builds, one locally patched instance and a remote model whose parameters changed without a new interface version. A closed-loop chain therefore begins with a controlled release identity: the smallest stable description that lets both institutions decide whether a later safety instruction concerns the deployed object.

This term is an analytical proposal, not vocabulary found in Article 5(5). Its legal support is indirect. It rests instead on what several provisions presuppose. Annex I requires lifecycle risk management and safe performance, which cannot operate on an object the institution is unable to delimit; the public declaration must carry the details needed to identify the device; present Article 5(5) ties manufacture to technical

https://doi.org/10.1017/err.2026.10167

documentation; and MDCG 2023-1 associates identification with tracking affected products and patients.[22] None of those sources expressly prescribes a release hash, lot hierarchy or recipient deployment key. The inference is functional: corrective action cannot be directed at an affected instance if the institutions cannot distinguish it from unaffected instances.

Commercial UDI materials supply a useful design analogy, not a hidden duty for exempt devices. The MDR and IVDR establish UDI systems for devices within their ordinary structures; Commission Implementing Decision 2019/939 designates issuing entities. MDCG materials distinguish the Basic UDI-DI from the device-specific UDI-DI, discuss changes that trigger a new identifier and place UDI governance inside the organisation's QMS.[23] The point is not that an in-house transfer must carry a UDI. Rather, the established system shows why family identity and production identity perform different work.

For the same reason, release identity must remain modality-sensitive. A physical instrument may require model, design revision, serial or batch, component state and manufacture date. For software, product name alone is rarely enough; version, build, validated configuration, dependencies and an immutable digest where technically suitable can matter. MDCG 2018-5 recognises that software identification turns on version changes, while the current software-qualification guidance separates medical-device software from software performing only storage, communication or simple search.[24] An assay may need method revision, reagent and calibrator lots, instrument settings and analytical acceptance limits. A patient-matched printed article may require the design revision, patient-input link, printer, material lot, build parameters and post-processing state. IMDRF's production-verification document for personalised medical devices provides a non-Union technical comparator for that last problem.[25]

2. *Acceptance is a recorded state, not a delivery receipt*

Once the object is fixed, the recipient must decide whether that release can be used in its own environment. This proposed acceptance stage is narrower than a conformity assessment and wider than proof of delivery: the record covers the received release, local infrastructure, interfaces, storage and handling, authorised use, user competence, validation result and any restrictions. A refusal or conditional acceptance is legally intelligible; silent installation is not a useful control state.

That distinction matters most for software and IVDs. MDCG 2023-4, addressing medical-device software used with hardware, calls for verification and validation of compatibility and

[22] MDR Art. 5(5)(e)(ii), (f)–(h) and annex I paras. 1–4; IVDR Art. 5(5)(f)(ii), (g)–(i) and annex I paras. 1–4; MDCG 2023-1 *supra*, note 9 9–12.

[23] MDR Arts. 27–9 and annex VI; IVDR Arts. 24–6 and annex VI; Commission Implementing Decision (EU) 2019/939 of 6 June 2019 designating issuing entities to operate a system for the assignment of Unique Device Identifiers (UDIs) in the field of medical devices [2019] OJ L149/73; Medical Device Coordination Group, "Guidance on BASIC UDI-DI and changes to UDI-DI" (MDCG 2018-1 Rev.4, April 2021) <https://health.ec.europa.eu/system/files/2021-04/md_mdcg_2018-1_guidance_udi-di_en_0.pdf> (last accessed 14 July 2026); Medical Device Coordination Group, "Guidance note integration of the UDI within an organisation's quality management system" (MDCG 2021-19, July 2021) <https://health.ec.europa.eu/document/download/64443e95-e1be-4ffd-80f7-9c6a1b0b99b6_en?filename=md_2021-19_en.pdf> (last accessed 14 July 2026).

[24] Medical Device Coordination Group, "UDI Assignment to Medical Device Software" (MDCG 2018-5, October 2018) <https://health.ec.europa.eu/system/files/2020-09/md_mdcg_2018_5_software_en_0.pdf> (last accessed 14 July 2026); Medical Device Coordination Group, "Qualification and classification of software – Regulation (EU) 2017/745 and Regulation (EU) 2017/746" (MDCG 2019-11 Rev.1, June 2025) <https://health.ec.europa.eu/latest-updates/update-mdcg-2019-11-rev1-qualification-and-classification-software-regulation-eu-2017745-and-2025-06-17_en> (last accessed 14 July 2026).

[25] International Medical Device Regulators Forum, "Personalized Medical Devices – Production Verification and Validation" IMDRF/PMD WG/N74 FINAL:2023 (11 April 2023) <https://www.imdrf.org/documents/personalized-medical-devices-production-verification-and-validation> (last accessed 14 July 2026).

https://doi.org/10.1017/err.2026.10167

interoperability across intended configurations and for communication mechanisms concerning changes and incidents.[26] MDCG 2020-1 likewise treats valid clinical association, technical performance and clinical performance as distinct parts of software evaluation.[27] Those documents concern ordinary regulatory settings and do not create a transfer-acceptance duty. They do, however, refute the idea that safe use follows from file identity alone.

At this stage, the private record must also make the release addressable. Addressability means that a safety instruction can reach every authorised deployment and that each deployment can return an execution status. Recipient legal identity is only the beginning. Beneath it lie the levels at which an instruction actually lands: site and department, then the instrument or software endpoint, then the stock location, and, where proportionate, the affected patient, specimen or result. Personal data should be stored only where needed and on a lawful basis; Article 5(1)(c) GDPR requires data minimisation, while health data receive the protection of Article 9.[28] The recommendation is therefore a linkable custody record, not an indiscriminate central patient list.

3. *Change control preserves the meaning of traceability*

A release identity becomes false if either institution changes the object while leaving the identifier untouched. Change control is thus no ornamental QMS entry; it preserves the proposition that the traced item remains the item assessed. The chain should distinguish an administrative correction, a technical change within the same release, a new release requiring acceptance, a safety correction requiring temporary cessation, and a recipient alteration amounting to modification or local manufacture. The converse rule matters equally. A change of supplier reference, internal document number or local label alone creates no new controlled release, and no institution may discharge an outstanding instruction by renaming what it holds.

Software makes the problem visible. A dependency patch may leave the intended purpose untouched but alter cybersecurity exposure. A model update may change output behaviour without changing the user interface. A receiver-side configuration script can make the deployed system differ from the transferor's validated build. MDCG and IMDRF materials treat security as lifecycle work, including communication, security-issue management and updates. Landman and colleagues documented a browser update that disrupted the link from an emergency-department tracking board to the radiology image viewer. Jabin's case report describes a patient-monitoring patching tool that signalled completion although about half the centres or clients patched the previous day still required a restart the next morning. Neither account concerns an Article 5(5) transfer or establishes patient injury; both show why the deployed clinical state must be checked after an update.[29] A software bill of materials can identify affected dependencies; it does not allocate legal responsibility.

[26] Medical Device Coordination Group, "Medical Device Software (MDSW) – Hardware Combinations: Guidance on MDSW Intended to Work in Combination with Hardware or Hardware Components" (MDCG 2023–4, October 2023) 6–8 <https://health.ec.europa.eu/system/files/2023-10/md_mdcg_2023-4_software_en.pdf> (last accessed 14 July 2026).

[27] Medical Device Coordination Group, "Guidance on Clinical Evaluation (MDR)/Performance Evaluation (IVDR) of Medical Device Software" (MDCG 2020-1, March 2020) 9–15 <https://health.ec.europa.eu/document/download/19d9e24f-2808-4e00-bfeb-75892047407d_en?filename=md_mdcg_2020_1_guidance_clinic_eva_md_software_en.pdf> (last accessed 14 July 2026).

[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (GDPR), Arts. 5(1)(c), 6 and 9.

[29] Medical Device Coordination Group, "Guidance on Cybersecurity for Medical Devices" (MDCG 2019-16 Rev.1, July 2020) 15–23 <https://health.ec.europa.eu/document/download/b23b362f-8a56-434c-922a-5b3ca4d0a7a1_en?filena

https://doi.org/10.1017/err.2026.10167

Change control also determines whether the original transfer remains the right legal description. MDCG 2023-1 treats manufacture broadly enough to include production from raw materials or components and combinations that create a new device; it separately states that a shared written protocol is not a device.[30] If the recipient substitutes a reagent, changes a design file or rebuilds software, the legal result depends on what changed, the intended purpose and the resulting product. No universal answer follows; the classification depends on what was transferred and on the conditions the receiving institution can meet. The record must instead expose the change so that the classification can be made on the facts.

4. An incident report is a trigger, not a completed response

Read at its exact level, the proposed recipient-to-transferor report moves information from the institution observing use to the institution associated with transfer, and no further. The sentence states no reporting period, required content, receipt confirmation, risk-classification method, authority route or fallback where the transferor is silent. Nor does it say that the recipient must wait before protecting its patients. These are omissions from the proposed interface, not proof that no other legal or professional duty applies. Those duties run within each institution rather than between them, and none of them generates a release-specific instruction that the other institution must acknowledge.

A workable trigger should carry the time, affected release, observed failure or result, immediate clinical consequence, evidence preserved and local interim measure. On receipt, the transferor needs to identify the controlled baseline and assess whether the signal concerns one deployment, every copy of a release, a component used across releases, or a recipient-side change. The ordinary vigilance framework offers a disciplined comparison, because it sequences what the proposal leaves unordered. Manufacturer awareness starts the reporting period. Investigation follows, competent authorities may intervene in it, and evidence in the device or batch must not be altered in a way that frustrates it.[31] Those provisions are not treated here as directly applicable to an exempt transfer. Their value lies in revealing the procedural questions left unanswered when the proposal says only that an incident is reported to the transferor.

Urgency changes sequence, not the need for control. Where continued use may expose patients to serious harm, the recipient must be able to suspend local use before the transferor completes root-cause analysis. Conversely, a technically informed transferor may detect a cross-recipient defect before any recipient reports an incident, yet the proposal contains no express forward safety-notice duty. An interface built only around backward incident information is reactive by design. The retained lifecycle duty gives an interpretive reason to communicate a discovered risk, but the obliged sender and the recipient's response should be stated rather than assumed.

---

me=md_cybersecurity_en.pdf> (last accessed 14 July 2026); International Medical Device Regulators Forum, "Principles and Practices for Medical Device Cybersecurity" IMDRF/CYBER WG/N60 FINAL:2020 (20 April 2020) <https://www.imdrf.org/documents/principles-and-practices-medical-device-cybersecurity>; International Medical Device Regulators Forum, "Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity" IMDRF/CYBER WG/N73 FINAL:2023 (13 April 2023) <https://www.imdrf.org/documents/principles-and-practices-software-bill-materials-medical-device-cybersecurity>, both (last accessed 14 July 2026). See also A. B. Landman and others, "The Hazard of Software Updates to Clinical Workstations: A Natural Experiment" (2013) 20 Journal of the American Medical Informatics Association e187, doi: 10.1136/amiajnl-2012-001494; Md S R Jabin, "Operational Disruption in Healthcare Associated with Software Functionality Issue Due to Software Security Patching: A Case Report" (2024) 6 Frontiers in Digital Health 1367431, doi: 10.3389/fdgth.2024.1367431.

[30] MDCG 2023-1 *supra*, note 9, 5–7.

[31] MDR Arts. 87 and 89(1)–(5); IVDR Arts. 82 and 84(1)–(5); MDCG 2023-3 Rev.2 *supra*, note 20 questions 14–15.

https://doi.org/10.1017/err.2026.10167

5. Use stops only when receipt becomes execution

A use-stop instruction should contain at least six elements: the affected release identity; the hazard and degree of urgency; the action to stop or restrict use; the evidence or item to preserve; any patient, specimen or result review; and the conditions, if known, for return to use. This is a recommendation. It draws by analogy from the content logic of MDR Article 89(8), IVDR Article 84(8) and the action range collected in MDCG 2023-3 Rev.2.[32] Electronic instructions can support rapid distribution, but availability is not reception. Even the ordinary electronic-instructions regime retains rules about access, version history and provision of paper information in specified circumstances.[33]

Acknowledgement closes that evidential gap. The recipient records when the instruction arrived, when access or use was blocked, which locations and instances were checked, what remained unresolved, and whether another institution had received the device. A response of "received" is inadequate if it does not state execution; equally, a transferor's outgoing email log cannot establish that a diagnostic workflow ended or a remote instance was disabled. The proposed chain therefore separates instruction, receipt and execution as different states.

Beyond execution, remediation is modality-specific. Physical stock may be quarantined, returned or destroyed; software disabled, updated or rolled back; an assay suspended and earlier results reviewed. For an implanted or patient-matched article, removal may be clinically worse than surveillance. Ordinary FSCA examples and IMDRF legacy-device guidance recognise that range.[34]

In the proposed lifecycle, custody closure requires an auditable account of every affected instance, including any open exception. That account should record whether access is blocked, corrected or expressly released; whether downstream recipients have responded; whether necessary patient or result action is recorded; and whether return, destruction or replacement is documented. Closure should allow stated exceptions: a device retained for investigation, an unreachable endpoint or a patient for whom removal is contraindicated remains an open item rather than disappearing into a completed-case label. Controlled resumption needs a new or confirmed release identity and a recipient acceptance decision, without which a temporary stop can decay into undocumented reuse. Figure 2 assembles these states into a release-to-closure lifecycle.

IV. Two institutions, one safety event

1. Technical knowledge and clinical control are divided

After transfer, neither institution alone necessarily controls the whole event. The manufacturing institution holds the design history, production record and comparative signals across releases; a transferor that is not itself the manufacturer may instead hold the custody record and recipient contact while lacking full technical authority. The receiving institution controls local access, clinical workflow, users, specimens, result communication and immediate patient protection. A rule assigning the whole response to one side will often assign part of it to the actor least able to perform it.

[32] MDR Art. 89(8); IVDR Art. 84(8); MDCG 2023-3 Rev. 2 *supra*, note 20 question 17.

[33] Commission Implementing Regulation (EU) 2021/2226 of 14 December 2021 laying down rules for the application of Regulation (EU) 2017/745 as regards electronic instructions for use of medical devices [2021] OJ L448/32, Arts. 5–7.

[34] MDCG 2023-3 Rev. 2 *supra*, note 20 20–2; International Medical Device Regulators Forum, "Principles and Practices for the Cybersecurity of Legacy Medical Devices" IMDRF/CYBER WG/N70 FINAL:2023 (11 April 2023) <https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices> (last accessed 14 July 2026).

https://doi.org/10.1017/err.2026.10167

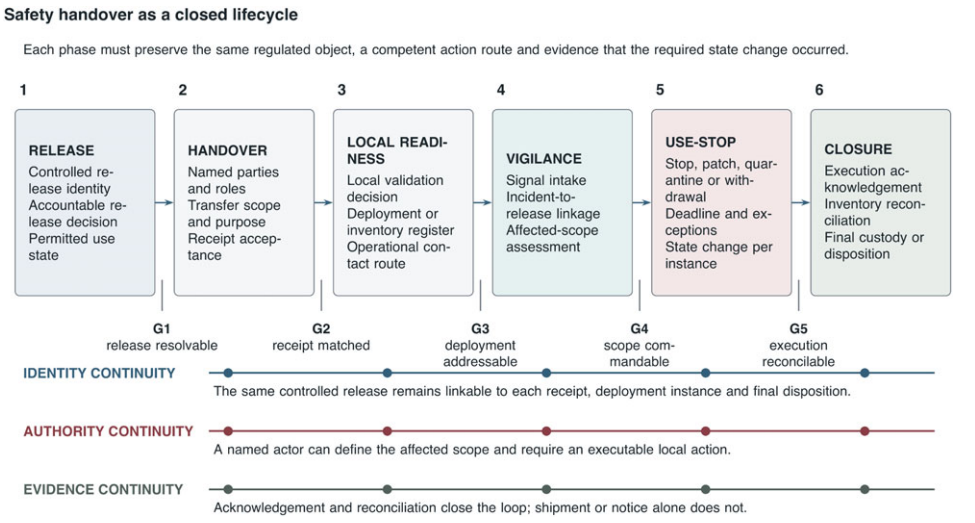


Figure 2. Author-proposed safety-handover lifecycle. Five gates test whether release, receipt, deployment, affected scope and execution can be resolved, matched, addressed, acted on and reconciled. The phases and gates are analytical recommendations, not conditions stated in COM (2025) 1023.

Alt text: Six phases run from release to closure. Five gates test the connecting record, while three lines require continuity of identity, authority and evidence.

Current Article 5(5) can refer simply to "the health institution" because point (a) prevents the legally relevant split. The proposal introduces "transferring" and "receiving" institutions only for traceability and incident reporting. It does not say whether the manufacturer and transferor must be identical, who owns the risk decision, or who tells the recipient to resume. Region Skåne's official consultation response identifies responsibility allocation and post-market requirements as matters needing clarification, with software and shared medical infrastructure as concrete boundary problems.[35] That response is not law. It confirms, however, that the ambiguity is perceived by a health-system operator rather than manufactured solely by doctrinal abstraction.

Allocated soundly, the response is concurrent and sequenced. On the transfer side, the institution controlling the manufacturing baseline assesses technical scope, links signals across recipients, issues a release-specific instruction and maintains the master correction record. Locally, the receiver triages the event, acts immediately where delay would expose patients, identifies deployments and affected clinical outputs, preserves evidence, executes the instruction and returns status. Neither role excludes competent-authority action under retained powers. The recommendation attaches a local control duty to the institution that actually permits use; it does not make the recipient a commercial manufacturer.

This minimum public-law allocation does not determine civil liability, professional discipline, contractual indemnities or data-controller status.

2. Silence, disagreement and non-response need a rule

The simple case is cooperative: the recipient reports a signal, the transfer side evaluates it, both agree on suspension, and every affected instance is located. A legal interface should

[35] Region Skåne, "Remiss Europeiska kommissionens förslag till översyn av det medicintekniska regelverket" (2026-POL000078, 26 March 2026) 3–4 <https://www.regeringen.se/contentassets/d79c8e7023fa46fb92388a96cb382b40/region-skane.pdf> (last accessed 14 July 2026).

https://doi.org/10.1017/err.2026.10167

be drafted for the harder cases. The transferor may regard the event as local misuse while the recipient suspects a release defect; the recipient may continue use because no substitute exists; contact details may be obsolete; a weekend emergency may arise before either governance committee can meet.

For immediate local risk, the recipient should have authority to suspend or restrict use without prior permission. That recommendation follows from control over the clinical setting and the retained Annex I baseline; it is not an express sentence in the proposal. The transfer side should then be informed and given the evidence needed for a wider assessment. Where the transferor issues a safety instruction, the receiver should either execute it or document a reasoned clinical exception with compensating measures and competent-authority escalation; an unreasoned refusal would break the chain.

Non-response should produce timed escalation rather than repeated informal messages. The final act could require current emergency contacts and acknowledgment within a risk-based period, leaving exact periods to subordinate material. Where acknowledgment does not arrive, the transferor should notify the relevant competent authority or authorities and the recipient's designated governance contact.

A cross-border transfer sharpens the same defect. Two national competent authorities may each hold inspection and restriction powers, yet the proposal assigns the exempt route no coordinating function. Ordinary vigilance law constructs that coordination expressly, obliging authorities to coordinate their assessments where a serious incident or a proposed field safety corrective action touches more than one Member State, under a coordinating authority anchored by default to the manufacturer's registered seat. That anchor does not translate. Two health institutions in different Member States have no manufacturer's seat to locate, and a bare traceability sentence supplies no substitute.[36]

V. Where the chain breaks

That allocation cannot be judged in the abstract: the proposed route must work for objects which differ markedly in how identity, use and correction are recorded. A serialised physical item is only one case, and the easiest. Software changes without moving at all. An assay drifts through a reagent lot or an instrument configuration that no transfer record ever named, while a design file yields as many objects as the recipient chooses to print. Emergency supply may run ahead of any complete local assessment, and the recipient may pass what it received onwards to an institution the transferor has never dealt with. The following examples are constructed legal tests, not reported incidents, and each asks the same five questions: what is the regulated object, which release is affected, where is it in use, what state change is required, and what evidence closes the event?

1. Software: correction without physical return

Institution A transfers build 4.2 of an in-house decision-support application to institutions B, C and D. The release passed local acceptance at all three. B later changed a configurable threshold; C installed build 4.2 on two virtual machines but retained build 4.1 for a specialist workflow; D allowed authenticated remote use by a separate legal entity. A then finds that build 4.2 can suppress a warning when a particular data field is null.

[36] MDR, Art. 89(9)–(11); IVDR, Art. 84(9)–(11). The coordinated procedure applies where concern arises about a serious incident or cluster relating to the same device or device type of the same manufacturer in more than one Member State, or where the appropriateness of a proposed field safety corrective action in more than one Member State is in question; unless the authorities agree otherwise the coordinating authority is that of the Member State of the manufacturer's registered place of business, and its designation does not displace the other authorities' own powers.

https://doi.org/10.1017/err.2026.10167

A family name cannot determine the affected population. Version alone may also fail because local configuration and dependencies can alter performance. Medical-software traceability literature accordingly treats version, machine and operating environment as separate identifiers, while Prictor's work on clinical decision support distinguishes the availability of a correction from its implementation by the user.[37] The release key in this example would have to resolve build 4.2 and any configuration relevant to the defect. The deployment record would identify each endpoint and the legal entity controlling it.

Return is the wrong physical model. Depending on risk and technical feasibility, local execution may mean disabling access, restoring a validated earlier build, applying a corrected build, changing a configuration, or restricting the intended use while a correction is assessed. Work on software-related device recalls shows why software faults may demand action even where no tangible product is collected.[38] Closure would require a response for every affected endpoint, including the remote deployment at D's downstream institution. A statement that three recipients received an email proves neither that four relevant deployments were found nor that each changed state.

AI-enabled devices need a further boundary. The proposal would move the Regulations from Section A to Section B of AI Act Annex I, limiting that Act through its Article 2(2). That move has not been made: the Digital Omnibus on AI, adopted in July 2026, effected the same transfer for machinery alone and left the medical-device entries in Section A. Device law and the AI Act therefore remain parallel regimes, subject to the AI Act's phased application: the high-risk requirements in Chapter III, Sections 1–3, for systems within Article 6(1) and Annex I apply from 2 August 2028. Even so, in-house software will not always be AI, meet Article 6(1)'s condition or fall within Annex III, and case-specific AI duties supply no general bilateral use-stop and acknowledgement route.[39]

2. *Other modalities: assay, printed object and onward transfer*

What holds for software holds, in different material, for the remaining transferable forms. Take an in-house IVD moved as a validated assay configuration, its handover record naming a method revision, instrument model, analytical software and specified reagents. During a shortage the receiving laboratory substitutes a reagent lot and recalibrates; results later disclose a bias confined to the combination of that substituted lot, one calibrator lot and one instrument software version. The affected object is a configuration rather than a name, and an instruction addressed to the assay alone would be at once too broad and dangerously narrow.

Additive manufacture divides the object again, and along a different seam. A hospital may send a finished printed device, disclose a design protocol, or provide a file from which the recipient manufactures its own object. These are not interchangeable events. MDCG 2023-1 distinguishes a written protocol from a product that meets the device definition; a

[37] Bianchini and others *supra*, note 6; Prictor *supra*, note 3.

[38] J. G. Ronquillo and D. M. Zuckerman, "Software-Related Recalls of Health Information Technology and Other Medical Devices: Implications for FDA Regulation of Digital Health" (2017) 95 The Milbank Quarterly 535, doi: 10.1111/1468-0009.12278.

[39] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024, Arts. 2(2), 6(1) and annex I; COM (2025) 1023 *supra*, note 2, Arts. 1(5)(b), 2(5)(b) and 4; Council ST 9801/26 *supra*, note 14 para 19. The move has not been effected: Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 (Digital Omnibus on AI), OJ L, 2026/1744, 24.7.2026, Art. 1(41), deletes point 1 of Section A and adds Regulation (EU) 2023/1230 on machinery to Section B, leaving the medical-device entries in Section A. Regulation (EU) 2026/1744, Art. 1(40), also amends AI Act Art. 113 to set 2 August 2028 as the application date for Chapter III, Sections 1–3, in respect of systems classified as high-risk under Art. 6(1) and annex I.

https://doi.org/10.1017/err.2026.10167

transfer analysis must first identify what crossed the boundary.[40] Hospital-makerspace research likewise reports both distribution of printed copies and disclosure of design files, illustrating the factual alternatives without deciding their legal classification.[41]

Onward movement, finally, removes the addressee altogether. Institution A transfers a device to B; B later passes a physical unit, assay access or software credentials to C, a legal entity with which A has never dealt. An incident at B prompts A to instruct B to stop use. C receives nothing because it is absent from A's record. Bilateral traceability between A and B is accurate yet incomplete for the affected population.

3. Emergency transfer: less time, not less identity

COM (2025) 1023 includes preparation for or response to a public-health emergency among the proposed grounds for a qualifying transfer.[42] Assume that a regional outbreak creates an immediate need for an in-house assay. The receiving institution cannot finish every local verification step before first use without defeating the clinical purpose.

Time pressure of that kind is the strongest objection to a detailed handover record, though not to the minimum chain, since urgency raises rather than lowers the cost of ambiguity. A staged acceptance can identify the provisional release, restricted intended use, authorised site, named contacts, unresolved local conditions, expiry or review time, and an immediate route to suspend use. Later steps may complete verification and reconcile instances created during the provisional period. The design does not treat emergency care as ordinary administration; it preserves the few facts without which a later correction cannot be directed.

VI. Drafting the missing connection

1. The binding act should carry the operative core

The final amending Regulation should state the duties that determine whether a safety instruction crosses the institutional boundary: release-level identification; reciprocal communication of a safety signal, correction or restriction; recipient action with execution acknowledgment and any justified exception; and retention of transfer, action and closure records for competent-authority access.

Traceability alone, on the other hand, cannot supply these duties. Union product law separates identification, safety communication and user action: MDR Article 89(8) and IVDR Article 84(8) require the notice to identify the device, explain the risk and state what users must do. Article 5(5) needs a shorter chain across institutions, but the missing links are the same.

What follows is offered as a drafting core for discussion, not as finished legislative text. It is set out in the form the act itself would take, recital before enacting terms, so that each rule can be argued with:

> (x) Where an in-house device is transferred between health institutions, the institution that manufactured it no longer controls the conditions of its use. Traceability records the movement of such a device, but does not by itself allow a safety decision to be addressed to the affected release, executed at the place of use and confirmed. Provision should therefore be made for the communication,

[40] MDCG 2023-1 *supra*, note 9 7–8.

[41] C. Rigtering, L. J. Spaans and J. P. J. de Jong, "How to Bridge the Nurse Innovation–Diffusion Gap? An In-Depth Case Study of Create4Care" (2023) 11 Frontiers in Public Health 1209965, doi: 10.3389/fpubh.2023.1209965.

[42] COM (2025) 1023 *supra*, note 2 Arts. 1(5), 2(5).

https://doi.org/10.1017/err.2026.10167

execution, acknowledgement and closure of safety measures between the institutions concerned, without extending to those institutions the obligations applicable to economic operators placing devices on the market.

In Article 5(5), the following subparagraphs are inserted after point (a):

1. Where a device is transferred under point (a), the health institution responsible for the manufacture of the device and for its technical documentation shall, without undue delay, notify each recorded receiving health institution of any safety correction, or of any instruction to cease or restrict use, concerning an identifiable transferred release.

2. Where the transferring institution is not the institution responsible for manufacture, it shall transmit that notification to its recorded recipients and relay their responses upstream.

3. A receiving health institution may suspend or restrict local use before receiving a notification under paragraph 1 where immediate patient protection so requires.

4. A receiving health institution shall: (a) identify the affected deployments and instances; (b) suspend, restrict, quarantine, correct, return or destroy each affected instance as the notified action class requires and in proportion to the risk; (c) acknowledge execution, or state a reasoned clinical exception which shall be documented, time-limited and notified to the competent authority; and (d) transmit the notification and the duties under this paragraph to every recorded subsequent recipient.

5. Where no acknowledgement is received within the period provided for under paragraph 7, the notifying institution shall inform the competent authorities of the Member States concerned. Deployments that are neither acknowledged nor reconciled shall remain open.

6. The institutions concerned shall record correction, return, destruction or resumption of use, and shall retain the transfer, action and closure records and make them available to the competent authorities on request.

7. The Commission may, by means of implementing acts, specify the record fields, message formats and response periods for the purposes of paragraphs 1 to 6.

Read against Table 1, each paragraph closes one of the gaps recorded there: paragraph 1 names the institution that must issue a release-specific instruction, paragraph 2 resolves the case in which manufacture and transfer are separated, paragraphs 3 and 4 place immediate protection and execution with the institution that controls use, paragraph 5 gives silence a consequence, and paragraph 6 makes closure visible to supervision.

The drafting is the author's, and two points are left deliberately open. "Transferred release" needs a formulation broad enough for software builds, IVD configurations and patient-matched articles; "resumption of use" cannot authorise a transferor to override national clinical law. Legislative counsel would integrate both with the final structure of the Regulations.

Within that structure, the final act should distinguish transfer eligibility from continuing duties. A late acknowledgment or incomplete closure record should not leave

https://doi.org/10.1017/err.2026.10167

the exemption's retrospective status unclear. Supervision, remediation and any penalty should be proportionate while preserving urgent authority powers.

Likewise, the term "incident" requires repair. A short provision could state that, for Article 5(5), incident carries the Article 2 content whether or not the transferred device was made available on the market. An alternative is a route-specific term such as "safety event," followed by criteria. Either is preferable to relying on an unexplained use of a market-linked definition, and any change must be made in binding text because it defines the trigger for a legal duty.

2. Delegated powers and common specifications are not a certain substitute

COM (2025) 1023 would confer power on the Commission to amend Annex I by delegated act in response to scientific or technical progress, international developments, emerging risks or technologies. Wider common-specification powers appear elsewhere in the instrument.[43] As drafted, the new Article 5 power speaks to the general safety and performance requirements in Annex I. By its terms, the provision does not authorise the Commission to create a bilateral recipient acknowledgement duty, decide onward-transfer legality or reallocate Article 5(5) responsibility between institutions. The Council progress report records that several proposed delegations remain under legal scrutiny.[44]

Article 290(1) TFEU supplies the sharper reason. The Court treats as essential those elements whose adoption requires political choices balancing divergent interests. Recipient execution, clinical exception, escalation and non-response allocate safety responsibility between independent institutions and should be enacted by the legislature. Technical fields and formats may follow later.[45]

The operative core should therefore be enacted in Article 5(5). Common specifications may later detail Annex I within a valid legal basis, but cannot supply the missing addressee and consequence.

By contrast with the technical detail, that distinction is one of competence. Articles 114 and 168(4)(c) TFEU support a common product-safety interface, while Article 168(7) preserves Member-State responsibility for the organisation and delivery of care.[46] The Union rule should identify the transferred release, safety message, acknowledgment and authority-accessible record. It should not determine the recipient's clinical treatment decision, patient-management choice or internal allocation of staff and resources, which remain governed by applicable national law.

3. Guidance should specify the record, not invent the duty

Once the duties exist, conversely, MDCG guidance may supply the modality-specific handover, use-stop and closure forms. Examples may translate the common states into software builds and endpoints, assay configurations and testing windows, patient-matched production records or physical stock. The minimum fields are those of Figure 3; no modality-specific field should become universal where it has no technical meaning.

Response periods should be risk-based. Guidance may propose default windows and escalation templates, subject to national authority powers. Patient- or specimen-linked records must comply with GDPR purpose limitation, data minimisation, security and the

[43] COM (2025) 1023 *supra*, note 2 proposed MDR Art. 5(7) and Art. 9(1), and proposed IVDR Art. 5(7) and Art. 9(1).

[44] Council ST 9801/26 *supra*, note 14 para 17.

[45] Consolidated Version of the Treaty on the Functioning of the European Union [2016] OJ C202/47, Art. 290(1); Case C-696/15 P *Czech Republic v Commission* EU:C:2017:595, paras. 75 and 78.

[46] Consolidated Version of the Treaty on the Functioning of the European Union [2016] OJ C202/47, Arts. 114, 168(4)(c) and 168(7); COM (2025) 1023 *supra*, note 2, explanatory memorandum, section 2.

https://doi.org/10.1017/err.2026.10167

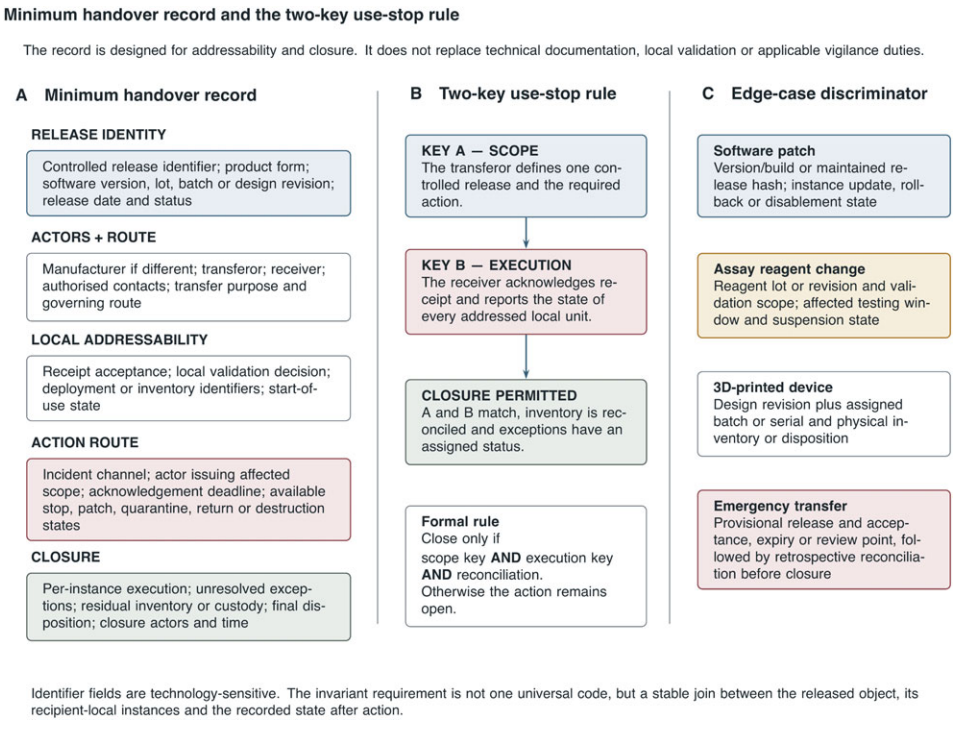


Figure 3. Author-proposed minimum handover record and two-key use-stop rule. Closure requires the transferor's affected-scope key to match the receiver's execution key, with inventory and exceptions reconciled. The displayed fields are modality-sensitive recommendations, not wording stated in the Commission proposal.
Alt text: Three panels list minimum record fields, match transferor scope to receiver execution, and distinguish software, assay, printed-device and emergency identifiers. Closure requires matching keys and reconciled exceptions.

rules for health data. A locally resolvable link may suffice; pseudonymisation remains processing and does not displace Articles 6 and 9, controller allocation or professional secrecy.[47]

4. A legal test for implementation

Judged properly, the proposed route is not tested by whether two institutions can produce a transfer document after the event. Its practical test is prospective and state-based: each stage must disclose whether it is complete, conditional or open. Can the transferor identify the exact release, has the recipient accepted it for a stated environment, and can every deployment be addressed? Does a material change produce a new status, can either side trigger an urgent stop, and does the recipient return execution evidence? Are unresolved instances visible, and is resumption or final disposal recorded?

Failure at one state should keep the chain open. A traceability record without a release key cannot support scoped correction; a notice without acknowledgment proves dispatch only; an acknowledgment without deployment reconciliation leaves unknown instances; destruction at B does not close custody if C received an onward copy. Figure 3 reduces the record to the two keys that must match, the transfer side's affected scope and the receiver's execution evidence, a test deliberately narrower than a QMS audit, asking only whether the legal bridge introduced by transfer can carry a safety decision to completion.

[47] GDPR Arts. 4(5), 5(1)(b)–(f), 6, 9 and 32.

https://doi.org/10.1017/err.2026.10167

Adoption of that minimum would not turn health institutions into ordinary economic operators or impose the entire vigilance chapter on the exempt route. It would do something more exact: connect the retained Article 5(5) duties to the institutional separation created by the new exception. Transfer may then remain exceptional, purpose-limited and supervised, while the law acquires a route by which use can actually be stopped.

VII. Conclusion: the event closes only when use has changed state

This article opened with an instruction that travelled and a use that did not stop. The proposed exception separates technical knowledge, custody and clinical control, and bilateral traceability with backward incident reporting does not establish that an affected release can be found, that an instruction reaches every deployment, or that use changes state. Ordinary recall law exposes those gaps without governing an Article 5(5) transfer.

A two-key use-stop follows. The institution controlling the technical baseline scopes the release and issues the instruction; the receiver executes, records justified exceptions and returns deployment-level evidence. Dispatch proves communication only.

The final Regulation should place release identity, reciprocal safety communication, execution acknowledgement and closure in Article 5(5), while resolving "incident" and onward transfer. Guidance may supply forms and periods, not the missing addressee or consequence.

Implementation turns on six recorded answers: affected release, deployment, actor able to stop it, action taken, unresolved instances, and the basis for resumption or custody closure. Otherwise the event remains open. What this article establishes is the executability of such a command, not the necessity of the exception that would make it required; whether the transfer route should be opened at all rests on evidence this article does not supply. If any of the six remains open, the safety event remains open.

Financial support. This research received no specific grant from any funding agency, commercial or not-for-profit sectors.

Competing interests. The author declares none.

Cite this article: A Peters, "A Transfer Route Without a Stop Route: Safety Execution Under the Proposed Article 5(5) Amendments to the MDR and IVDR". *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2026.10167

https://doi.org/10.1017/err.2026.10167