Ref. Ares(2025)11508145 - 22/12/2025

Call: HORIZON-HLTH-2022-TOOL-11

Topic: HORIZON-HLTH-2022-TOOL-11-02

Funding Scheme: HORIZON Research and Innovation Actions (RIA)

Grant Agreement no: 101095435

Deliverable No. 2.1

Manuscript on MDR, IVDR and AI Act

Contractual Submission Date: 31/12/2025

Actual Submission Date: 22/12/2025

Responsible partner: P8: UNIWARSAW

Funded by
the European Union

Grant agreement no.	101095435
Project full title	REALM - Real-world-data Enabled Assessment for heaLth regulatory decision-Making

Deliverable number	**D2.1**
Deliverable title	**Manuscript on MDR, IVDR and AI Act**
Type	Report
Dissemination level	Public
Work package number	WP2
Work package leader	P08-UNIWARSAW
Author(s)	Dominika Harasimiuk Tomasz Braun
Keywords	AI Act, MDR/IVDR, Legal compliance, AI medical devices, AI Regulation

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HaDEA).

Neither the European Union nor the granting authority can be held responsible for them.

Document History

Version	Date	Description
V01	1.12.2025	D2.1 Ready for review
V02	15.12.2025	Reviewed by Emad Yaghmaei
V03	15.12.2025	Reviewed by Emanuele Ratti
V04	22.12.2025	D2.1 After integrating remarks of reviewers is ready for submission

Table of Contents

List of Abbreviations and definitions

AI - Artificial Intelligence

AIB - European Artificial Intelligence Board

CAPA - corrective or preventive actions

CEN – Comité Européen de Normalisation

CENELEC - Comité Européen de Normalisation Electrotechnique

CIBCB - Conference on Computational Intelligence in Bioinformatics and Computational Biology

CJEU - Court of Justice of the European Union

CS - common specifications

DPIA – data protection impact assessment

EDPB - European Data Protection Board

EHDS - European Health Data Space

ETSI - European Telecommunication Standards Institute

EU - European Union

EUDAMED - European Database on Medical Devices

FRIA – fundamental rights impact assessment

FSCA - field safety corrective actions

GDPR - General Data Protection Regulation

GSPR - General Safety and Performance Requirement

HDAB - Health Data Access Bodies

IEC - International Electrotechnical Commission

ISO - International Organisation for Standarisation

IVDR - In Vitro Diagnostic Regulation

JTC - Joint Technical Committee

MDAI - medical devices with AI

MDCG - Medical Device Coordination Group

MDR - Medical Devices Directive

NCA - national competent authorities

NLF - New Legislative Framework

PMCF - post-market clinical follow-up

PMPF - post-market performance follow-up

PSUR - periodic safety update reports

QMS - quality management systems

1 Executive Summary

Artificial intelligence is reshaping healthcare by introducing adaptive, data-driven technologies into medical devices, diagnostics, and clinical workflows. Because AI systems rely on continuous learning and the large-scale processing of sensitive health data, their integration into medical technologies has prompted the EU to build a layered regulatory framework involving the Artificial Intelligence Act (AI Act), the General Data Protection Regulation (GDPR), and the Medical Device and In Vitro Diagnostic Regulations (MDR/IVDR). This Deliverable, produced within WP2 of the REALM project, offers an integrated analysis of how these regimes jointly apply to AI in the medical-devices sector.

The study has three main objectives. First, it maps the obligations imposed on key actors—manufacturers, providers, deployers, operators, controllers, and processors—highlighting where terminology differs but responsibilities converge across the AI Act, MDR/IVDR, and GDPR. Second, it examines how horizontal (AI Act, GDPR) and sector specific (MDR/IVDR) regulations interact in practice, identifying areas of complementarity as well as risks of fragmentation. Guidance from bodies such as the MDCG and the forthcoming AIB is considered essential for ensuring coherent interpretation. Third, the analysis assesses the practical impact of this regulatory environment on innovation, market access, and healthcare delivery, with particular attention to the obligations of healthcare institutions deploying AI systems.

Methodologically, the study draws on binding EU legislation and relevant soft-law instruments, applying a comparative and teleological interpretation to clarify overlaps and divergences. Because all four regulations have extraterritorial reach, their obligations extend to non-EU actors whose AI systems affect EU patients. A functional comparative approach further shows how legal requirements translate into conformity assessment, quality-management processes, and post-market surveillance duties.

2 Introduction and Methodology

2.1 Objective and scope of the Deliverable

The rapid proliferation of artificial intelligence (AI) in healthcare presents a regulatory challenge of unprecedented complexity[1]. Unlike traditional medical technologies, AI systems are characterised by adaptability, autonomy, and reliance on large-scale datasets, often encompassing sensitive health and genetic information. Their integration into medical devices, diagnostics, and healthcare services has compelled European regulators to respond with a layered normative framework, one that draws on multiple legal instruments simultaneously: the Artificial Intelligence Act (AI Act)[2], the General Data Protection Regulation (GDPR)[3], the Medical Device Regulation (MDR)[4], and the In Vitro Diagnostic Regulation (IVDR)[5]. The present study, being a research work performed within WP2 "Ethical, Legal and Societal Framework" of the REALM project, situates itself at the crossroads of these legal regimes, aiming to offer a comparative and integrative analysis of their application to AI systems in medical devices sector. The legal analysis of the fast changing regulatory environment concerning AI technologies applicable in medical devices sector in the EU is one of the objectives of the WP2 (O2.2) which was achieved through the work performed within the Task 2.2 (Analysis of legal frameworks adopted at the EU level (MDR, IVDR, Proposal for the AI act) and selected EU member states).

The objective of the research performed within the Task 2.2, which resulted in the present Deliverable is threefold. First, to map the obligations of key stakeholders involved in the lifecycle of AI in medical devices sector, namely manufacturers, providers, deployers, and operators. In our analysis we will try to align the terminology of abovementioned acts, which even if it shows some differences, yet is rooted in the logic of the New Legislative Framework (NLF) approach, underpinning EU market regulation[6]. The AI Act, for instance, identifies the "provider"[7] of an AI system as the central actor responsible for compliance with high-risk AI requirements, while the MDR and IVDR employ the notion of "manufacturer"[8] with a similar, though not identical, scope. Parallelly, the GDPR designates "controllers" and

[1] C. Menella et al., 'Ethical and regulatory challenges of AI technologies in healthcare: A narrative review' (2024) 10 Heliyon e26297 doi: 10.1016/j.heliyon.2024.e26297

[2] 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) [2024] OJ L 2024/1689.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) [2016] OJ L119.

[4] 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 (MDR) [2017] OJ L117/1.

[5] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission decision 2010/227/EU (IVDR) [2017] OJ L117/176.

[6] S. du Boispéan, M. Mueck, Ch. Gaie, Introduction to the European New Legislative Framework, in M. Mueck, Ch. Gaie (eds) 'European Digital Regulations' (Springer 2025) 1-19 https://doi.org/10.1007/978-3-031-80809-8

[7] Art. 3 point 3 of the AI Act.

[8] Art. 2 point 30 of the MDR, art. 2 point 23 of the IVDR.

"processors" as the principal entities accountable for lawful data processing[9]. By aligning these regulatory terminologies, the study seeks to clarify the overlapping and sometimes diverging duties imposed on stakeholders across legal acts.

Second, the study examines the interplay between the different layers of EU regulation. The AI Act introduces a horizontal risk-based framework applicable across sectors, while the MDR and IVDR impose vertical, sector-specific safety and performance requirements on medical technologies. GDPR applies transversally, governing the processing of personal and health-related data that inevitably underpins both the development and deployment of AI in healthcare. The simultaneous application of these regimes raises the risk of fragmentation or duplication of compliance duties. Accordingly, this analysis explores the mechanisms of coordination and complementarity that can be identified in the legislative texts themselves, as well as in interpretative guidance issued by bodies such as the Medical Device Coordination Group (MDCG) and the European Artificial Intelligence Board (AIB).

Third, the comparative scope of the study extends beyond purely doctrinal analysis. By focusing on the position of manufacturers , providers, deployers, and operators, it seeks to assess how the regulatory framework impacts innovation, market access, and clinical practice, with the major focus on the medical devices sector. Particular attention is given to the role of healthcare institutions as "deployers" of AI systems and the obligations this entails in relation to transparency, accountability, and oversight. In terms of scope, this study is confined to the European Union, with a primary emphasis on binding legal acts and adopted policy guidance. The study is not limited to theoretical alignment but aims to provide practical insights into how these regulations intersect in real-world healthcare settings, shaping responsibilities, compliance strategies, and ultimately, patient safety and fundamental rights.

2.2 Methodological approach: legal sources and interpretative guidance

The methodological approach adopted in this study is grounded in a legal-comparative analysis that integrates both binding secondary EU legislation and soft law measures that serve as an interpretative guidance issued by competent authorities. The complexity of regulating AI in the medical devices sector stems from the coexistence of horizontal and sector-specific frameworks, each with its own legal terminology, scope, and enforcement mechanisms. A systematic methodology is therefore necessary to identify overlaps, divergences, and complementarities across the AI Act, GDPR, MDR, and IVDR.

At the foundation of the analysis lies reliance on secondary EU law measures, namely regulations. The choice of this legislative tool by EU institutions allows for the direct applicability, direct effect of their

[9] Art. 4 points 7 and 8 of the GDPR.

provisions, as well as the extraterritorial scope of their application[10]. The AI Act establishes a horizontal regime for AI systems based on risk classification and lifecycle obligations. The AI Act entered into force in 2024. Its formal entry into force opened the two-year period during which the provisions of the AI Act will be phased in. The Regulation shall apply from 2 August 2026, however part of its provisions regarding general rules and prohibited AI practices as well as general-purpose AI, governance mechanisms and penalties are applicable since 2 February and 2 August 2025 respectively. The most relevant provisions for the medical devices sector, namely the core framework regarding high-risk AI systems[11] and corresponding provisions, will be applied thirty-six months after entry into force (August 2027), giving the necessary time for harmonised standards, notified bodies, and technical infrastructure to mature. However, under the recent Digital Omnibus proposal, more flexibility is envisaged by linking the entry into application of the provisions regarding high-risk AI systems to the availability of the harmonised standards. It means that once standards are adopted, the Commission may decide to make the rules applicable earlier, without creating a blanket 36-month delay[12]. The MDR and IVDR, applicable since 2021 and 2022 respectively, provide vertical, sector-specific requirements for medical devices and in vitro diagnostic devices. Even if the AI powered medical devices are not mentioned in these regulations as such, it is understood that broad definition of medical device and in vitro medical device covers such devices incorporating AI technologies. The GDPR, effective since 2018, applies across sectors and regulates all processing of personal data, including health data, forming the indispensable legal backdrop against which healthcare AI systems are developed and deployed. Our decision to include the reflection on the GDPR into the scope of this Deliverable, results from the fact that this act, governing the personal data protection in the EU plays fundamental role in the AI medical devices sector. Explaining interdependencies not only between AI Act, MDR and IVDR, but also between these acts and GDPR adds extra layer of scientific reflection.

It should be stressed that in case of GDPR and AI Act the extraterritorial scope of application is introduced directly in their respective provisions[13]. For GDPR it means that it is applicable not only to EU-based controllers and processors but also to non-EU entities offering services to EU patients. Article 3 GDPR provides that the Regulation applies to the processing of personal data in the context of the activities of an establishment in the Union, regardless of whether the processing takes place within the EU. More significantly, Article 3.2 extends applicability to non-EU controllers and processors where they either offer goods or services to data subjects in the Union or monitor their behaviour within the Union.

[10] L. Hornkohl, 'The Extraterritorial Application of Statutes and Regulations in EU Law' (February 16, 2022) MPILux Research Paper 2022(1), available at SSRN: https://ssrn.com/abstract=4036688 or http://dx.doi.org/10.2139/ssrn.4036688

[11] Art. 6.1 of the AI Act.

[12] European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on Artificial Intelligence (Digital Omnibus on AI), COM(2025) 836 final 9.

[13] See art. 3 of the GDPR and art. 2.1 a) and c) of the AI Act.

Similarly, for the AI Act, the extraterritorial scope of application results from provisions stating that it encompasses providers that place AI systems or general-purpose AI models on the Union market irrespective of their geographical establishment. The AI Act captures providers and deployers established in third countries when the outputs of their AI systems are utilised within the Union.

This extraterritorial reach ensures that global technology companies developing healthcare AI, even when based outside the EU, fall within the AI Act and GDPR if their systems are placed on the EU market and deployed for EU patients.

The comparative method entails a structured reading of these texts against one another, guided by the New Legislative Framework (NLF) principles. By aligning the roles of "providers" under the AI Act, "manufacturers" under MDR/IVDR, and "controllers/processors" under GDPR, the analysis reveals how actors positioned differently in each framework nevertheless converge in terms of regulatory obligations. This interpretative mapping is designed not merely to juxtapose obligations but to demonstrate functional equivalence and practical interdependence.

A second methodological pillar is the reliance on soft law measures, which will include interpretative guidance, references to standards and policy documents. Regulatory texts of the EU rarely operate in isolation; they are supplemented by detailed guidance intended to promote uniform implementation across Member States. For the MDR and IVDR, this role is performed by the Medical Device Coordination Group (MDCG), which issues non-binding but influential documents on classification, clinical evaluation, and qualification of software. Particularly relevant is MDCG 2019-11[14], clarifying when software falls within the definition of a medical device. For the AI Act, interpretative authority is vested in the AIB, which will support the Commission and the AI Office by publishing guidelines, recommendations, and opinions to facilitate coherent enforcement[15]. Issuing of such documents is essential, as their function will likely mirror that of the Article 29 Working Party and subsequently the European Data Protection Board (EDPB) under the GDPR, whose opinions and guidelines have become authoritative interpretative sources in practice[16].

The methodology also integrates teleological and systemic interpretation. Because the AI Act, GDPR, MDR, and IVDR pursue overlapping but distinct regulatory objectives, respectively, trustworthy AI, data protection, patient safety, and device performance, their provisions must be read in light of their broader regulatory purposes. Teleological interpretation ensures that provisions are not reduced to their literal wording but considered in terms of their underlying protective functions. For example,

[14] MDCG 2019-11 Rev.1, Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 –IVDR (October 2019, June 2025 rev.1). <https://health.ec.europa.eu/latest-updates/update-mdcg-2019-11-rev1-qualification-and-classification-software-regulation-eu-2017745-and-2025-06-17_en?prefLang=pl> accessed 1.10.2025.

[15] See art. 65 and 66 of the AI Act.

[16] C. J. Hoofnagle, B. van der Sloot, & F.Z. Borgesius, 'The European Union general data protection regulation: what it is and what it means' (2019) 28(1) Information & Communications Technology Law 96–97. https://doi.org/10.1080/13600834.2019.1573501

while the AI Act imposes obligations concerning dataset quality to mitigate bias, the GDPR's principles of lawfulness, fairness, and proportionality address similar concerns from the standpoint of data subjects' rights.

Finally, the study employs a functional comparative lens, moving beyond the formal scope of legal texts to consider how obligations translate into real-world compliance structures. This includes examining conformity assessment pathways, quality management systems, and post-market surveillance obligations that, while regulated under distinct instruments, converge in practice for manufacturers, providers and healthcare institutions operating AI-enabled systems.

In sum, the methodology combines doctrinal analysis of primary sources, reliance on interpretative guidance, and comparative mapping of roles and obligations across legal regimes. This approach ensures both conceptual clarity and practical relevance, enabling a comprehensive understanding of the regulatory environment governing AI in the medical devices sector.

2.3 Stakeholders in focus: manufacturers, providers, deployers, operators, controllers and processors.

A central challenge in assessing the regulatory framework for AI in the medical devices sector lies in the heterogeneous terminology employed by different EU instruments. Each regulation designates actors in ways that reflect its underlying objectives: market access, safety, or data protection. For this reason, a comparative mapping of stakeholders is necessary to clarify who is responsible for compliance, liability, and governance at each stage of the AI powered medical device lifecycle.

The AI Act places the "provider" at the centre of responsibility. Defined as 'a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge'[17], the provider is subject to extensive lifecycle obligations, including quality management, conformity assessment, post-market monitoring, and incident reporting. In practice, providers in the medical devices sector may range from large multinational technology companies to start-ups developing niche diagnostic tools. The AI Act further distinguishes "deployers," understood as a natural or legal persons, public authorities, agencies or other bodies who use AI systems in the course of their professional activity[18] (e.g., hospitals implementing diagnostic support software), and an overarching category of "operators," which includes providers, product manufacturers, deployers, authorised representatives, distributors, and importers[19]. It should be noted that the definition of operator covers product manufacturers, being a distinct notion from providers. Under the AI Act product manufacturers are understood as being part of the AI value chain. As is explained in the recital 87 of the AI Act, if a high-risk AI system serves as a safety component of a product covered by sectoral Union harmonisation legislation under the NLF (for example by the MDR or IVDR) and is not marketed or used separately from that

[17] Art. 3 point 3 of the AI Act.
[18] Art. 3 point 4 of the AI Act.
[19] Art. 3 point 8 of the AI Act.

product (for example medical device whose safety component is AI based solution), then the product manufacturer, as defined in that legislation, must fulfil the obligations of a provider under AI Act. In particular it concerns ensuring that the AI system integrated into the final product meets all the requirements laid down in the AI Act[20]. This layered approach reflects the NLF logic, where compliance responsibilities extend across the supply chain.

The personal scope of MDR/IVDR delineates the range of actors who bear obligations and responsibilities in the regulatory ecosystem governing medical technologies within the European Union. Similarly to the AI Act, by defining a series of "economic operators," the MDR/IVDR establish a chain of accountability extending from the original manufacturer to the final distributor, thus ensuring that every stage of a device's lifecycle is subject to regulatory oversight. At the core of this framework stands the manufacturer, defined as a "natural or legal person who manufactures or fully refurbishes a device or has a device designed, manufactured or fully refurbished, and markets that device under its name or trademark"[21]. This definition reflects the principle of regulatory attribution: the entity placing the device on the market under its brand assumes primary legal responsibility for its conformity with the MDR/IVDR. The inclusion of the element of "fully refurbishing" within the manufacturer's scope, which is understood as the complete rebuilding of an existing device or creation of a new one from used components, illustrates the regulation's attempt to adapt to a circular economy logic while preserving patient safety through the assignment of a new device lifetime.

Complementing the manufacturer's role, the MDR/IVDR recognises a network of other economic operators. These include:

- the authorised representative, established within the Union, mandated to act on behalf of a manufacturer based outside the EU;
- the importer, responsible for placing devices from third countries on the Union market; and
- the distributor, who makes a device available in the supply chain up to the point of putting it into service[22].

Together, these actors form an interdependent compliance chain, where obligations cascade according to each operator's proximity to the device's design, placement, and use. The MDR/IVDR also distinguishes health institutions, whose primary purpose is patient care or public health promotion, and users, including both healthcare professionals and lay persons, thereby extending the scope of the Regulation to the ultimate operational context of devices[23]. Functionally, terms of provider (AI Act) and manufacturer (MDR/IVDR) concentrate regulatory responsibility at the point of market entry, requiring the entity to establish a quality management system, compile technical documentation, undergo conformity assessment, and ensure post-market surveillance. For AI-enabled medical software, the provider under the AI Act and the manufacturer under MDR/IVDR will typically be the same entity.

[20] See recital 87 of the AI Act and art. 25. 3 of the AI Act.
[21] See art. 2 point 30 of the MDR; art. 2 point 23 of the IVDR .
[22] See art. 2 points 32-35 of the MDR; art. 2 points 25-28 of the IVDR.
[23] See art. 2 points 36-37 of the MDR; art. 2 points 29-30 of the IVDR.

As it was mentioned above, it is due to the fact that, where a high-risk AI system is a safety component of a product regulated under MDR/IVDR and is not placed on the market separately, the medical device manufacturer assumes the obligations of a provider under the AI Act.

As far as the use of AI systems is concerned, the AI Act introduces the concept of the *deployer*, defined as a "natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity"[24]. In healthcare, this includes hospitals, clinics, and laboratories that integrate AI into clinical practice. The MDR and IVDR, however, use the term *user* to denote the professional or lay person who uses a medical device in accordance with its intended purpose. While superficially similar, these roles are not identical. The deployer is an institutional actor, often responsible for ensuring transparency, human oversight, and proper use of the AI system, while the user may be an individual clinician or technician operating the device. Thus, in a hospital setting, the institution qualifies as a deployer under the AI Act, while the physician interacting directly with the software constitutes the user under MDR/IVDR.

In the GDPR, stakeholder terminology shifts from market and product focus to data governance. A fundamental principle of European data protection law, enshrined in the GDPR is the differentiation between the roles of "data controller" and "data processor"[25]. The data controller is the natural or legal person who determines the purposes ("why") and means ("how") of processing personal data[26]. The data processor processes personal data on behalf of the controller and according to the controller's documented instructions[27]. The GDPR thus places primary responsibility for lawful, fair, and transparent data processing on the controller, who must ensure compliance with all relevant data protection obligations. In practice, controllers make key strategic decisions such as which categories of patient or user data will be collected by a medical device, the duration of data storage, or the purposes for which those data may be shared with third parties (e.g. for clinical evaluation, algorithmic retraining, or regulatory reporting). Processors perform operational tasks under the controller's authority. For example, a cloud service provider hosting telemetry data from a wearable cardiac monitor, or a data analytics firm contracted to process sensor data for diagnostic pattern recognition.

It is also possible for two or more actors to act as joint controllers, where they jointly determine the purposes and means of processing[28]. For instance, a hospital and a medical device manufacturer may be joint controllers if both define how patient data collected via a connected insulin pump are used for treatment optimisation and device improvement. In such cases, the GDPR requires a clear allocation of responsibilities between the parties through a transparent arrangement.

[24] Art. 3 point 4 of the AI Act.
[25] M. Hintze, 'Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR' (June 7, 2018) Journal of Internet Law, Available at SSRN: http://dx.doi.org/10.2139/ssrn.3192721 accessed 23.10.2025; R. Becker, A. Thorogood, J. Bovenberg, C. Mitchell, A. Hall, 'Applying GDPR roles and responsibilities to scientific data sharing'(2022) 12 International Data Privacy Law 209–211, https://doi.org/10.1093/idpl/ipac011.
[26] Art. 4 point 7 of the GDPR.
[27] Art. 4 point 8 of the GDPR.
[28] Art. 26 of the GDPR.

A frequent source of confusion in both legal and technical practice arises from conflating the notion of the data controller with that of the data owner. While ownership typically refers to property rights or contractual entitlement to access and use data, control under the GDPR refers to the ability to decide why and how personal data are processed. The two concepts may overlap but are not identical. For example, in the medical device ecosystem:

- A patient may be regarded as the data owner of physiological data generated by a wearable health tracker, since the data originate from their body and pertain to their health.
- The device manufacturer, which defines how the device collects, stores, and transmits those data, acts as the data controller for the processing operations necessary to deliver the device's functionality.
- A cloud hosting provider or AI analytics subcontractor that processes the data to detect anomalies or improve diagnostic accuracy would be a data processor, acting under the instructions of the manufacturer (controller).

This distinction is essential, as regulatory accountability attaches to the controller regardless of data ownership. A manufacturer may process data it does not own but remains fully responsible under the GDPR for ensuring that such processing complies with data protection principles, including lawful basis, data minimisation, and purpose limitation.

Within the framework of the MDR/IVDR and AI Act, these distinctions acquire additional complexity. Manufacturers of AI-enabled medical devices often act as data controllers for personal health data processed by the device or its associated digital platform. Hospitals or clinical research partners may simultaneously act as joint controllers when defining clinical purposes or validation activities. Meanwhile, technology suppliers, such as algorithm developers or infrastructure providers, typically qualify as processors.

Unlike the AI Act and MDR/IVDR, where responsibilities flow with the product, the GDPR attaches obligations to decision-making power over data. Understanding and correctly mapping these roles is crucial for ensuring both regulatory compliance and ethical data governance. In an increasingly data-driven medical technology landscape, clarity on who determines the purposes, who performs the processing, and who holds ownership or access rights to the underlying data is indispensable for transparent accountability and trust in digital health systems.

The adopted comparative perspective reveals both alignment and divergence. Providers under the AI Act and manufacturers under MDR/IVDR share functional equivalence, with responsibility at the point of market entry. GDPR's controller/processor distinction cuts across these roles, potentially designating both providers and deployers as controllers depending on their data practices. Deployers under the AI Act, such as hospitals, face a dual regulatory identity: as deployers responsible for transparent and safe use of AI systems, and as data controllers under GDPR. Similarly, clinicians operating AI tools ,classified as "users" under MDR/IVD, may not bear primary compliance obligations, but their professional conduct is essential to ensuring that providers and deployers meet their regulatory duties.

For healthcare actors, this alignment means that a single institution or company may simultaneously embody multiple regulatory identities. A hospital introducing AI-based diagnostic software may be a deployer under the AI Act, a user under MDR/IVDR, and a controller under GDPR. Likewise, a technology company producing AI-enabled imaging software is at once a provider (AI Act), a manufacturer (MDR), and a controller for training datasets (GDPR). Understanding these cross-regulatory concepts is therefore critical to ensuring compliance across overlapping legal regimes. Identifying stakeholders across frameworks underscores a core theme of this study: obligations are distributed across multiple actors, and compliance in healthcare AI cannot be reduced to a single entity. Instead, effective governance depends on coordination between manufacturers, providers, deployers, and operators, each of whom embodies different regulatory identities across the AI Act, GDPR, and MDR/IVDR.

2.4 Interplay of EU regulations in AI medical devices sector

As already mentioned above, the regulation of AI in the medical devices sector cannot be understood by reference to a single legislative act. Instead, it is shaped by the simultaneous and complementary application of: the AI Act, the GDPR, and the two pillars of the NLF for medical technologies, the MDR and IVDR. Each of these regimes pursues distinct regulatory objectives, yet their scope overlaps significantly in the healthcare context. As a result, AI systems in this domain and their development, deployment, and operation are subject to a multi-layered framework that must be read in an integrated manner.

The AI Act establishes a horizontal regime applicable to AI systems across all sectors. Its central mechanism is a risk-based classification, with most AI systems used in healthcare qualifying as “high-risk” by virtue of being safety components of medical devices or in vitro diagnostics[29]. High-risk designation triggers stringent requirements, including conformity assessment and CE marking procedures aiming at verification of compliance of a given system with requirements set in Chapter III, Sect. 2 of the AI Act covering the obligations to establish risk management system, data governance practices, to keep appropriate technical documentation, assure record keeping, as well as to meet the requirements of transparency, human oversight, accuracy, robustness and security. Also, the high-risk AI systems providers are obliged to assure post-market monitoring and be subject to post-market surveillance. Importantly, the AI Act is designed to complement rather than replace sectoral regulations such as the MDR and IVDR, meaning that medical AI systems are subject to dual compliance obligations, yet run in uniform procedures.

The MDR and IVDR provide vertical, sector-specific regulation of medical devices and diagnostics. They focus on safety, clinical or performance evaluation, and post-market monitoring and surveillance, ensuring that products placed on the market achieve their intended medical purpose without exposing patients to disproportionate risks. AI-enabled systems that meet the definition of a medical device or in vitro diagnostic must therefore comply fully with MDR/IVDR requirements, including CE marking and conformity assessment by notified bodies.

[29] Art. 6.1 of the AI Act. H. van Kolfschooten, J. van Oirschot, ‘The EU Artificial Intelligence Act (2024): Implications for healthcare‘ (2024) 149 Helath policy 105152.

The GDPR cuts across both frameworks by regulating the processing of personal and health data underpinning AI development and deployment. AI system providers and manufacturers rely on large datasets for training and validation, while deployers (e.g., hospitals) process sensitive patient data in real-world use. GDPR principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality[30] apply irrespective of device classification or AI risk level. Moreover, GDPR introduces distinct obligations such as conducting Data Protection Impact Assessments (DPIAs) for high-risk processing and ensuring enforceable rights for data subjects. In practice, GDPR obligations attach not only to providers but also to deployers and healthcare professionals, creating a transversal layer of compliance.

The interplay of these instruments therefore creates both synergies and challenges. On the one hand, the AI Act explicitly recognises MDR/IVDR compliance mechanisms and allows documentation requirements to be integrated, reducing duplication[31]. On the other hand, overlapping obligations risk creating uncertainty, particularly in areas such as post-market surveillance and incident reporting, where MDR/IVDR and AI Act procedures must be coordinated. Similarly, GDPR duties relating to transparency and accountability interact closely with the AI Act's requirements for human oversight and transparency, demanding careful harmonisation at the institutional level.

Ultimately, the regulatory interplay reflects a layered governance strategy. The MDR and IVDR secure medical safety and performance; the GDPR guarantees protection of fundamental rights in data processing; and the AI Act addresses the unique risks of algorithmic decision-making. For medical devices sector stakeholders, compliance therefore requires an integrated approach that accounts for the cumulative and not alternative application of these legal frameworks.

3 Conceptual Framework and Legal Definitions of Key Notions

3.1 Definition of AI systems under the AI Act and its scope in the medical devices sector

The AI Act introduces, for the first time in EU law, a binding legal definition of an "artificial intelligence system." Article 3.1 defines an AI system as:

"a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"

This definition codifies inference as the central characteristic of AI systems: they do not merely process or compute but generate outputs by inferring patterns, correlations, or solutions from input data. It

[30] P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, (Springer 2017) 87-92.
[31] Art. 8.2 of the AI Act.

explicitly recognises both autonomy and adaptiveness as variable features of AI systems. These clarifications respond to criticisms that the initial proposal of the AI Act risked capturing overly broad categories of software while also failing to reflect the distinctive technical risks posed by learning systems[32].

The emphasis on inference is of particular significance for medical devices sector. Medical AI applications frequently produce outputs in the form of predictions (e.g., likelihood of disease progression), recommendations (e.g., treatment pathways), or decisions (e.g., triage prioritisation). They may also generate diagnostic or clinical content, such as image segmentations in radiology or genomic variant annotations in personalised medicine. By focusing on the inferential nature of these outputs, the AI Act ensures that even where clinicians retain the final decision-making authority, the AI tool itself is subject to regulatory scrutiny because of its capacity to shape clinical reasoning.

The definitional elements of autonomy and adaptiveness are equally central. Autonomy in this context is not absolute independence from human oversight, but the ability of the system to function without step-by-step programming once deployed. In healthcare, this includes, for example, AI systems embedded in medical imaging devices that automatically highlight regions of concern for further review. Adaptiveness, meanwhile, refers to the system's ability to alter or refine its functioning through learning, whether in development (training and validation) or post-deployment (continuous or self-learning)[33]. While adaptive capacity offers opportunities for more personalised care, it poses regulatory challenges: systems may evolve beyond the parameters originally assessed, raising questions of ongoing conformity and clinical safety.

The scope of the AI Act's definition of AI system is deliberately broad and technology-neutral[34]. This is how the paradigm of future-proof regulation is supposed to be achieved. The definition encompasses rule-based expert systems as well as machine learning and deep learning models. For healthcare, this inclusivity ensures that both "traditional" decision-support systems, which encode clinical guidelines, and advanced data-driven tools, which learn from vast patient datasets, fall under regulatory oversight. The breadth of the definition also extends to AI integrated into medical devices and diagnostics under the MDR and IVDR, thereby ensuring alignment between the horizontal AI framework and sector-specific device regulation.

At the same time, the definitional inclusivity may generate borderline cases. For example, software tools used in hospital administration or resource allocation may technically meet the definition of an AI system due to their inferential processes, even if their direct clinical relevance is limited. Here, the

[32] F. Vainionpää, K. Väyrynen, A. Lanamaki, A. Bhandari, 'A Review of Challenges and Critiques of the European Artificial Intelligence Act (AIA)' (2023) *Rising like a Phoenix: Emerging from the Pandemic and Reshaping Human Endeavors with Digital Technologies ICIS 2023,* 5 <https://aisel.aisnet.org/icis2023/aiinbus/aiinbus/14> access 13.11.2025.

[33] 'The concept of 'AI system' under the new AI Act: Arguing for a Three-Factor Approach' in: *Commission Guidelines on the Application of the Definition of an AI System and the Prohibited AI Practices Established in the AI Act. Response of the European Law Institute* (2024 Vienna) 12-14. <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_on_the_definition_of_an_AI_System.pdf> access 13.11.2025.

[34] A. Ojanen, 'Technology Neutrality as a Way to Future-Proof Regulation: The Case of the Artificial Intelligence Act'(2025) European Journal of Risk Regulation 1–2. doi:10.1017/err.2025.10024.

subsequent provisions of the AI Act, particularly the risk-based classification in its Articles 5–7, operate as filtering mechanisms, distinguishing high-risk clinical applications from lower-risk or purely administrative tools.

The adopted definition of an AI system reflects a functional approach that prioritises the inferential capabilities of systems, coupled with their potential autonomy and adaptiveness. In healthcare, this captures the full spectrum of AI applications influencing diagnosis, treatment, and patient management.

It should be borne in mind that the AI Act distinguishes AI system from general-purpose AI model, understood as "an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market"[35]. While AI systems, in particular the ones with high risks are subject to stringent regulatory measures, the general-purpose AI enjoy more relaxed requirements, and do not fall under the conformity assessment mechanisms. Most AI medical devices will not qualify as general-purpose AI models within the meaning of the AI Act, unless a GPAI model is placed on the market independently and later integrated into a medical device.

3.2 Personal data and health data under GDPR

The GDPR provides the primary legal framework for the processing of personal data in the European Union, including their use in the healthcare sector. Any assessment of AI in healthcare and in the medical devices sector in particular, must therefore begin with the definitional architecture of the GDPR, which sets the boundaries for lawful processing of patient and clinical information.

Personal data is defined in Article 4 point 1 of the GDPR as "any information relating to an identified or identifiable natural person (data subject)." The breadth of this definition has been consistently affirmed by the Court of Justice of the EU (CJEU), which has stressed that identifiability must be interpreted expansively, encompassing both direct and indirect means of identification[36]. In practice, this means that virtually all patient-related information processed in healthcare, from electronic health records and imaging files to metadata associated with wearable devices, falls within the scope of personal data.

[35] Art. 3 point 65 of the AI Act.
[36] CJEU judgment of 19 October 2016, *Breyer* (C-582/14, EU:C:2016:779); CJEU judgment of 4 September 2025, *EDPS v SRB* (C-413/23 P, ECLI:EU:C:2025:645).

Within this broad category, the GDPR recognises specific subtypes of data that warrant heightened protection because of their sensitivity. Most significant for healthcare is the category of data concerning health, defined as personal data "related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."[37] Recital 35 of the GDPR provides explanation of this definition, clarifying that it encompasses any data gathered while registering for or receiving cross-border health services, any identifier assigned to someone for medical purposes, information obtained from examining the body or its samples (including genetic material), and all details about a person's health status, such as illnesses, disabilities, risks, medical history, treatments, or physiological conditions, regardless of whether it comes from a doctor, hospital, medical device, or laboratory test. The scope is thus not confined to clinical settings: data produced by fitness trackers, mobile health applications, or even AI-based lifestyle monitoring tools may qualify as health data when linked to individual wellbeing.

Closely linked are two other sensitive categories: genetic data and biometric data**.** Genetic data is "personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person."[38] Given the growing role of AI in genomic medicine and personalised therapeutics, the legal qualification of genetic data is critical. Biometric data is defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person."[39] In healthcare, biometric systems may include facial recognition tools for patient identification or gait analysis used in neurological diagnostics.

All three categories: health, genetic, and biometric data, are at the same time classified under Article 9 GDPR as "special categories of personal data," subject to a general prohibition on processing. Processing is permissible only under limited exceptions[40]. They include among others, explicit consent by data subject, pursuit of vital interests of data subject, significant public interest, health-care–related needs, like preventive or occupational and medicine, preventing cross-border threats to public health or scientific research. It should be stressed that exceptions set in art. 9.2 of the GDPR should be interpreted narrowly and their catalogue is closed. This heightened level of protection reflects the potential harms associated with misuse: discrimination, stigmatisation, and breaches of fundamental rights to privacy and dignity.

The ways to mitigate the risks related to personal data processing is to apply anonymisation or pseudonymisation techniques[41]. Anonymisation and pseudonymisation constitute two distinct approaches to reducing identifiability in personal data processing, yet they differ fundamentally in both purpose and legal effect. Anonymisation refers to an irreversible process through which all identifiers (direct and indirect) are removed or transformed to the extent that re-identification of the data subject is no

[37] Art. 4 point 15 of the GDPR.
[38] Art. 4 point 13 of the GDPR.
[39] Art. 4 point 14 of the GDPR.
[40] Art. 9.2 a-h of the GDPR.
[41] R. Tinabo, F. Mtenzi and B. O'Shea, 'Anonymisation vs. Pseudonymisation: Which one is most useful for both privacy protection and usefulness of e-healthcare data' (2009) International Conference for Internet Technology and Secured Transactions, (ICITST), London, UK 1-6, doi: 10.1109/ICITST.2009.5402501.

longer reasonably possible using any means likely to be employed by the controller or third parties. Once data is effectively anonymised, it falls outside the scope of the GDPR. In contrast, pseudonymisation involves replacing identifying elements with artificial identifiers or codes while retaining the ability to re-identify individuals through separately stored additional information[42]. Pseudonymised data remain personal data under the GDPR, albeit with reduced risk profiles and often enabling more flexible use within appropriate technical and organisational safeguards. In practice, anonymisation supports truly privacy-preserving secondary use, whereas pseudonymisation enables controlled linkage and analysis while maintaining accountability and data subject protections. In light of the recent CJEU's case law there is a certain level of relativity as it concerns differences between pseudonymised and anonymised data. According the CJEU position in *EDPS v SRB* case "pseudonymised data must not be regarded as constituting, in all cases and for every person, personal data for the purposes of the application of Regulation 2018/1725 (GDPR), in so far as pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable."[43]

For AI in healthcare, these definitions have immediate consequences. Training and validation datasets typically contain health and genetic data, while real-world deployment often requires continuous processing of sensitive information about patients. As a result, nearly all stages of the AI lifecycle engage Article 9 GDPR restrictions, making data governance and lawful basis determination central to compliance strategies. It is understood that even seemingly anonymised datasets may re-enter the scope of personal data if re-identification risks persist[44].

3.3 Notions of Medical device and in vitro diagnostic software under MDR/IVDR

The legal qualification of AI-based software as a medical device or in vitro diagnostic medical device is central to determining its regulatory pathway in the European Union. The MDR and the IVDR, both of which entered into application in 2021 and 2022 respectively, provide detailed statutory definitions that frame the scope of regulatory oversight for health technologies.

I Under Article 2 point 1 MDR, a medical device is defined as:

> "any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:
> — diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
> — diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,

[42] Art. 4 point 5 of the GDPR.
[43] Par. 86 of the case C-413/23 *EDPS v SRB* (n 36).
[44] See, Art. 29 DATA PROTECTION WORKING PARTY, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216.

> — investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
> — providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations,
> and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.
> The following products shall also be deemed to be medical devices:
> — devices for the control or support of conception;
> — products specifically intended for the cleaning, disinfection or sterilisation of devices as referred to in Article 1(4) and of those referred to in the first paragraph of this point."

Importantly, the definition explicitly includes software, provided that it is intended for one of these medical purposes. This clarification, reinforced by Recital 19 MDR, resolves earlier debates under the former Medical Devices Directive[45] as to whether stand-alone software could qualify as a medical device. For AI systems, the intended purpose declared by the manufacturer is determinative: software used to support clinical decision-making, diagnose disease from imaging, or predict patient deterioration will fall within the scope of the MDR[46]. Conversely, software with purely administrative or lifestyle functions, such as staff rostering or general wellness tracking, lies outside this definition.

The IVDR adopts a parallel but distinct approach for diagnostic technologies. Article 2 point 2 IVDR defines an *in vitro diagnostic medical device (IVD)* as:

> "any medical device which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, whether used alone or in combination, intended by the manufacturer to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information on one or more of the following: concerning a physiological or pathological process or state; concerning congenital physical or mental impairments; concerning the predisposition to a medical condition or a disease; to determine the safety and compatibility with potential recipients; or to predict treatment response or reactions."

Here, too, software is expressly included in the legal definition. AI-enabled applications for genomic interpretation, digital pathology, or biomarker analysis fall within the IVDR when their outputs provide diagnostic, prognostic, or predictive information based on in vitro examination of human specimens.

The crucial element that needs to be taken into consideration while qualifying medical devices or IVD is their intended purpose. This means that classification is determined not by the product's objective function, but by the purpose the manufacturer claims in the labelling, instructions for use, or advertis-

[45] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices [1993] OJ L 169/1.
[46] M. Ebers, 'AI Robotics in Healthcare Between the EU Medical Device Regulation and the Artificial Intelligence Act. Gaps and Inconsistencies in the Protection of Patients and Care Recipients' (2024) 11 Oslo Law Review 3-4.

ing materials. Consequently, a product may in fact be suitable for medical use, yet it will not be classified as a medical device if the manufacturer does not present it as such[47]. Both regulations make clear that medical device (or IVD) software, including AI, refers to software intended, on its own or together with other products, to fulfil a purpose falling within the MDR or IVDR definitions of a medical device or an IVD. This applies regardless of the fact if the software operates independently or serves to drive or influence the functioning of another device[48]. The scope is intentionally broad to ensure that emerging technologies are captured even where their material embodiment is limited to code and algorithms. The MDCG has provided further clarification in its Guidance 2019-11, confirming that software which performs actions on or for the benefit of individual patients, based on medical information, qualifies as a device under MDR/IVDR[49]. As it was confirmed by the CJEU[50], still under provisions of Medical Devices Directive, which was repealed by the MDR, software, of which at least one of the functions makes it possible to use patient specific data for the specific medical purposes is, in respect of that function, a medical device, even if that software does not act directly in or on the human body. By contrast, software performing purely organisational tasks or supporting general health and well-being without a specific medical purpose is excluded.

Systematising types of medical device software, it can be classified according to its relationship with hardware and its intended user. From a hardware perspective one can distinguish independent and combined medical device software. Independent has its own medical purpose and operates on general-purpose hardware. Combined fulfils its purpose only when paired with hardware providing essential input data; it may be embedded within a medical device or function as a separate app communicating with external devices or using built-in sensors[51]. Some software used with medical devices does not qualify as medical device software. Programs that operate or influence a hardware device, such as user interfaces or software that reports device status, are treated as components or accessories and remain within the scope of the MDR/IVDR, but they are not classified as medical device software[52]. A second classification criterion concerns the end user. Medical device software may be designed for healthcare professionals or for laypersons.

For AI systems in healthcare abovementioned definitions have profound consequences. Classification as a medical device or IVD triggers the full set of regulatory obligations under MDR or IVDR, including conformity assessment, clinical or performance evaluation, post-market surveillance, and CE marking. Moreover, because most AI applications in healthcare are intended to influence diagnosis, monitoring,

[47] Ibid.
[48] MDCG 2019-11 rev. 1 (n 14).
[49] Ibid.
[50] CJEU judgment of 7 December 2017, *Syndicat National de l'Industrie Des Technologies Medicales (Snitem)* (Case C-329/16, ECLI:EU:C:2017:947). See commentary to this judgement, T. Minssen, M. Mimler, 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 621-623.
[51] P. Minghetti et al, 'Patient-managed digital medical devices: Do we need further regulation?' (2024) 47 Informatics in Medicine Unlocked https://doi.org/10.1016/j.imu.2024.101506
[52] Ibid.

or treatment, they will typically fall within these definitions, positioning them within the strictest tier of EU product regulation[53].

4 Material Scope of Applications and Classification

4.1 Risk-based classification under the AI Act (prohibited, high-risk, limited, acceptable)

The AI Act aims at introducing harmonised rules for the placing on the market, the putting into service, and the use of AI systems in the Union, as well as prohibiting certain AI practices.

The regulatory concept of the AI Act is structured around a risk-based approach, reflecting the principle that legal obligations should be proportionate to the potential risks posed by AI systems to selected key values such as health, safety, and fundamental rights.[54] The AI Act introduces a graduated system of obligations corresponding to four principal categories: prohibited AI practices, high-risk AI systems, systems subject to limited risks with transparency obligations and acceptable risks AI systems.[55]

Prohibited AI practices. The AI Act sets out a narrow list of practices that are considered unacceptable because they contravene Union values and fundamental rights.[56] These include, inter alia, AI systems deploying subliminal techniques that materially distort behaviour in a way likely to cause harm; systems exploiting the vulnerabilities of children or persons with disabilities; and certain forms of real-time remote biometric identification in publicly accessible spaces, subject to strict law enforcement exceptions. While the primary focus is not on healthcare, the prohibitions are relevant for example for the systems that could manipulate vulnerable patients into unsafe health-related decisions. The prohibition of social scoring by public authorities also serves as a safeguard against discriminatory access to healthcare services based on algorithmic profiling.

High-risk AI systems. The core of the AI Act is the regulation of high-risk AI systems designation of which arises either because the AI is a safety component of a product regulated under EU product safety law, or because it is listed in Annex III as high-risk in itself.[57] In healthcare, this category captures nearly all clinically relevant AI, since AI-enabled medical devices and in vitro diagnostics fall under the MDR and IVDR, as they usually are safety components or products subject to third-party conformity assessment under these sectoral regulations As a result, diagnostic imaging software, predictive analytics tools for intensive care, or AI systems interpreting genetic data will qualify as high-risk. Such systems are subject to stringent obligations, including risk management, quality management systems,

[53] D.Onitiu, S. Wachter, B. Mittelstadt, 'How AI challenges the medical device regulation: patient safety, benefits, and intended uses' (2024) Journal of Law and the Biosciences, lsae007, https://doi.org/10.1093/jlb/lsae007
[54] M. Ebers, 'Truly Risk-based Regulation of Artificial Intelligence. How to Implement the EU's AI Act'. (2025) European Journal of Risk Regulation, 16(2), 684–703. doi:10.1017/err.2024.78
[55] M. Gille, M. Tropmann-Frick and T. Schomacker, 'Balancing Public Interest, Fundamental Rights, and Innovation: The EU's Governance Model for Non;''-High-Risk AI Systems', Internet Policy Review (2024) 13(3).
[56] Art. 5 of the AI Act.
[57] Art. 6.1 read in conjunction with Annex I and art. 6.2 read in conjunction with Annex III of the AI Act.

technical documentation, conformity assessment, and continuous post-market monitoring. High-risk systems must also meet requirements relating to data governance, transparency, human oversight, robustness, accuracy, and cybersecurity.[58]All these requirements will be further elaborated below.

Limited-risk and transparency obligations. A third category includes systems with limited risk, to which the AI Act applies only minimal obligations, primarily transparency duties[59]. In healthcare, limited-risk systems might include AI-driven administrative assistants or scheduling tools, which do not directly affect clinical decision-making but nonetheless interact with patients or staff. While these systems are not high-risk, transparency remains essential to maintain trust in patient-facing interactions.

Acceptable-risk AI systems. The vast majority of artificial intelligence systems currently available on the European market fall into the low, acceptable risk category. These are solutions that do not pose significant risks to the health, safety or fundamental rights of users. Examples include recommendation algorithms for online shops, content personalisation applications and text and image editing support systems. In their case, the AI Act does not impose mandatory compliance or registration requirements, recognising that the potential risk is minimal and does not justify a full regulatory regime. However, this does not mean complete freedom. The Act encourages providers of such systems to take voluntary self-regulatory measures, which may take the form of codes of conduct, internal quality standards, and other mechanisms to increase transparency and accountability.

Healthcare implications. The practical effect of the risk-based framework in the healthcare sector is that most clinically significant AI applications will fall into the high-risk category. As a consequence, it triggers extensive compliance duties.[60] The prohibitions resulting from the unacceptable or high risk classifications serve as a backstop against ethically forbidden uses. Limited-risk obligations are intended to ensure transparency in patient interactions outside of core medical treatment. Lower-risk tools are let to be developed with minimal burdens. In all cases life-critical AI is subject to rigorous oversight.

4.2 Scope of the MDR/IVDR and device classification rules

The MDR establishes a comprehensive regulatory framework governing the placing on the market, making available on the market, and putting into service of medical devices and their accessories intended for human use within the Union, while simultaneously extending its scope to clinical investigations conducted in the EU. In addition, the Regulation applies, upon the adoption of common specifications pursuant to Article 9, to the product groups without an intended medical purpose listed in Annex XVI. This extension is calibrated to the state of the art, drawing in particular on harmonised standards developed for technologically analogous medical devices[61].

[58] Art. 8–15 of the AI Act.
[59] Art. 50 of the AI Act.
[60] R. Kilian, L. Jäck, D. Ebel, 'European AI Standards-Technical Standardisation and Implementation Challenges under the EU AI Act' (2025) European Journal of Risk Regulation, 1-25.
[61] Art. 1.1-2 of the MDR.

The classification of devices under the MDR and the IVDR is a decisive factor in determining the applicable conformity assessment procedures, the involvement of notified bodies, and the level of scrutiny which a medical device is subject to. For AI-enabled technologies, classification is not merely a technical exercise, but it directly influences the regulatory burdens placed on developers and healthcare institutions.

4.2.1 Medical devices under MDR.

The MDR establishes four risk-based classes of medical devices: Class I, IIa, IIb, and III**,** arranged in ascending order of risk. Classification is governed by Annex VIII, which provides detailed rules based on the intended purpose, invasiveness, duration of use, and potential impact on patients[62].

- *Class I* includes low-risk devices such as non-invasive monitoring software with limited clinical significance. These products may often rely on self-declaration of conformity, without the intervention of a notified body.
- *Class IIa and IIb* capture medium- to higher-risk devices, including many software applications that drive or influence diagnosis or therapeutic decisions. For example, AI-powered applications that process imaging data to identify pathologies are generally classified at least IIa, reflecting their potential to inform clinical judgment.
- *Class III* applies to the highest-risk devices, typically those that are life-sustaining or life-supporting, or that present a high potential for serious health impact if they malfunction. AI integrated into implantable devices or systems informing critical therapeutic interventions could fall into this category.

As far as it concerns software, the MDR provides specific rules of classification.[63] Software intended to provide information used for diagnostic or therapeutic purposes is classified as Class IIa, unless such decisions may cause death or irreversible deterioration (Class III) or lead to serious deterioration (Class IIb). This provision is of particular importance for AI-driven diagnostic systems, as it ensures that most clinically relevant software is placed in the higher-risk categories requiring notified body assessment.

4.2.2 In vitro diagnostic devices under IVDR.

The IVDR delineates the regulatory conditions governing the placing on the market, making available on the market, and putting into service of in vitro diagnostic medical devices and their accessories intended for human use within the Union. Its scope further encompasses performance studies carried out in the EU, thereby integrating both pre-market and investigational activities into a unified oversight framework. Through this dual focus, the Regulation ensures that analytical and clinical performance considerations are subject to consistent EU-level requirements throughout the device's lifecycle.

The IVDR adopts a different but equally risk-based classification scheme, structured into Classes A, B, C, and D, with Class A representing the lowest risk and Class D the highest. The classification rules, set

[62] MDCG 2021-24, Guidance on classification of medical devices (October 2021).
[63] Rule 11, Annex VIII of the MDR.

out in Annex VIII of the IVDR, are based on the intended medical purpose, the risk to individuals and public health, and the nature of the information provided by the device.

- *Class A* devices include low-risk laboratory equipment and certain software with limited diagnostic significance.
- *Class B* encompasses general diagnostic tests with moderate risk.
- *Class C* includes tests that provide information essential for patient management, such as companion diagnostics or infectious disease detection. Many AI systems that analyse genetic, molecular, or tissue data for diagnostic purposes fall into this category.
- *Class D* represents the highest risk, covering devices intended to detect life-threatening transmissible agents (e.g., HIV, hepatitis viruses) in blood or organ donations. AI-enabled systems assisting in the interpretation of such tests would therefore be classified as Class D.

4.2.3 Implications for AI in healthcare.

For AI-enabled medical software, MDR Annex VIII Rule 11 and the IVDR classification rules mean that low-risk classifications are the exception rather than the norm. Most clinically significant AI systems fall within Class IIa or higher under MDR, or Class C/D under IVDR. This classification has substantial regulatory consequences: manufacturers must undergo rigorous conformity assessment involving notified bodies, maintain detailed technical documentation, and implement comprehensive quality and post-market surveillance systems.

The classification rules thus function as a gatekeeping mechanism, ensuring that the level of regulatory scrutiny is commensurate with the potential impact of AI systems on patient health and safety. For manufacturers, accurate classification at the outset is essential, as misclassification may delay market entry or result in non-compliance. For healthcare institutions, the classification determines the assurances of safety and performance upon which clinicians and patients must rely.

4.3 Role of the GDPR in health-related data processing contexts

As was discussed above, the GDPR's scope of application is covering personal data. The GDPR in healthcare strengthens the role of patients as active rights-holders attributed to them in order to assure adequate level of personal data protection. Key rights include:

- **Access:** patients may request information about whether their data is being processed and obtain a copy[64].
- **Rectification:** inaccurate data must be corrected[65].

[64] Art. 15 of the GDPR.
[65] Art. 16 of the GDPR.

- **Erasure:** data subjects may request deletion, subject to exceptions for healthcare provision and legal obligations[66].

- **Restriction and portability:** patients may control how their data is shared or transferred, including between healthcare providers[67].

- **Right to object:** patients may object to certain forms of processing, particularly where data is used for research or secondary purposes[68]. However, as it concerns secondary use of data for research purposes the right to object does not work if the processing is necessary for the performance of a task carried out for reasons of public interest.

Healthcare institutions deploying AI must ensure that these rights can be meaningfully exercised, including in contexts where AI systems operate with complex or opaque data architectures.

The healthcare sector is particularly sensitive under the GDPR because most data processed qualifies under art. 9 of the GDPR as *special categories of personal data*, namely health, genetic, or biometric data. As noted in Point 3.2 above, processing such data is in principle prohibited unless falling under specific exceptions, including processing necessary for healthcare provision, for reasons of public interest in public health, or for scientific research subject to appropriate safeguards. AI developers and deployers must therefore ground their activities in one of these lawful bases and implement technical and organisational measures ensuring proportionality, necessity, and data minimisation.

4.3.1 Data protection by design and Data Protection Impact Assessments (DPIAs).

AI systems deployed in healthcare will often be considered as "likely to result in high risk to the rights and freedoms of natural persons"[69]. This, apart from the regular record of processing activities (ROPA), triggers the requirement for a Data Protection Impact Assessment (DPIA), which obliges controllers to systematically evaluate risks, consult with data protection officers, and, in some cases, supervisory authorities[70]. A DPIA must describe the processing, assess its necessity and proportionality, identify risks, and outline mitigation measures. Article 25 of the GDPR mandates "data protection by design and by default," requiring that privacy safeguards such as pseudonymisation, minimisation, and access restrictions be embedded directly into AI systems.

4.3.2 Global significance.

The GDPR shapes healthcare AI well beyond the EU's borders, functioning as a global benchmark[71]. Developers outside the EU seeking to market AI-enabled medical software to the European Union's healthcare institutions must build GDPR compliance into their systems. This reinforces the EU's

[66] Art. 17 of the GDPR.
[67] Art. 18 and 20 of the GDPR.
[68] Art. 21 of the GDPR.
[69] Art. 35 of the GDPR.
[70] See, M. Corrales Compagnucci, A. Dahi, and P.A Earls Davis, 'Conducting a Data Protection Impact Assessment in Health Science: A Comprehensive Guide' (November 10, 2023). Available at SSRN: https://ssrn.com/abstract=4651993 or http://dx.doi.org/10.2139/ssrn.4651993
[71] C. Ryngaert, and M. Taylor, 'The GDPR as Global Data Protection Regulation?'(2020) 114 AJIL Unbound 5–9. doi:10.1017/aju.2019.80

position as a normative power in digital health governance, introducing its standards of data protection and patient rights internationally.

4.4 MDCG/AIB guidance on overlaps and dual qualification

The regulation of AI in healthcare exemplifies one of the most complex issues of EU law: dual qualification, whereby a single product may simultaneously fall under multiple legal regimes with cumulative obligations. AI-enabled medical software frequently qualifies both as a *medical device* or *in vitro diagnostic medical device* under the MDR/IVDR and as a *high-risk AI system* under the AI Act. To ensure consistency, the European legislature and expert bodies such as the MDCG and AIB have sought to clarify how these regimes interact and avoid contradictory requirements[72].

As was discussed above, MDCG has issued influential interpretative documents clarifying when software, including AI-driven applications, qualifies as a medical device. Most notable is *MDCG 2019-11*, which states that software intended to provide information for diagnosis, prevention, monitoring, prediction, prognosis, treatment, or alleviation of disease should be considered a medical device[73]. This guidance ensures that AI tools influencing individual patient management, such as imaging analysis algorithms or predictive analytics systems, are brought within the MDR/IVDR scope. Importantly, MDCG has emphasised that qualification depends on intended purpose, and not on whether the software operates autonomously or merely supports clinical decision-making. Thus, even decision-support AI that does not directly act on the patient but informs physician judgment typically qualifies as a regulated device.

A medical device AI system qualifies as a high-risk AI system under Article 6.1 of the AI Act when two cumulative criteria are fulfilled: first, the AI system functions as a safety component of a medical device or constitutes a medical device in its own right; and second, it falls within the scope of a third-party conformity assessment conducted by a notified body pursuant to the MDR or IVDR. Such solution excludes from the scope of high-risk AI systems, medical devices falling under class I (non-sterile, non-measuring, non-reusable surgical) as well as IVD class A (non-sterile) for the reasons that for both categories there is no involvement of notified body. Similarly in-house devices according to Art. 5.5 MDR/IVDR are excluded[74].

Such a systemic interrelation creates an explicit legal bridge: once an AI system qualifies as a medical device or IVD, it is simultaneously captured by the AI Act's high-risk category. As a result, dual qualification is not an accidental overlap but a deliberate regulatory design. This ensures that healthcare AI systems are subject both to sector-specific safety and performance requirements (MDR/IVDR) and to horizontal safeguards addressing algorithmic risks (AI Act), such as robustness, bias mitigation, transparency, and human oversight. These regulatory requirements will be discussed below.

To avoid duplication, the AI Act provides mechanisms for integration. Article 8.2 allows providers of high-risk AI systems that are also medical devices to incorporate AI Act documentation into the

[72] AIB 2025-1 MDCG 2025-6, Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA), June 2025.
[73] See, n 14.
[74] AIB 2025-1 MDCG 2025-6, 6 (n 72).

MDR/IVDR technical files, provided all requirements are covered. Similarly, conformity assessments performed by notified bodies under MDR/IVDR must also consider compliance with the AI Act[75]. This integrated approach reflects the NLF logic, streamlining regulatory processes while maintaining the cumulative application of obligations. The details of compliance alignment in the context of dual classification under AI Act and MDR/IVDR will be further discussed in point 8.3 below.

5 General regulatory requirements for AI medical devices. Obligations of manufacturers and providers.

5.1 General remarks on regulatory requirements

The obligations imposed on manufacturers and providers of AI in the medical devices sector are structured around the principle of lifecycle regulation, ensuring that compliance is not limited to the moment of market placement but extends across design, development, and post-market phases. This approach is rooted in the NLF and is the reflection of concern about the availability in the EU single market of products which may cause harm to the society (mostly to health, safety and fundamental rights). Both the AI Act and the MDR/IVDR embed detailed requirements on design control, technical documentation, traceability, and instructions for use. Together, these obligations form the backbone of preventive regulatory oversight, anchoring accountability in the provider/manufacturer from the earliest stages of system development. The AI Act in its chapter III section 2 enlists regulatory requirements for high-risk AI systems, which are applicable also to AI medical devices[76]. These requirements must be integrated during design and development, in the pre-market (ex-ante), but also they need to be safeguard in the post-market (ex post) phases. These include:

- robust risk management system[77],
- appropriate data governance management practices[78],
- drawing and keeping technical documentation[79],
- record-keeping[80],
- transparency and provision of information to deployers[81],
- human oversight mechanisms[82],
- accuracy, robustness and cybersecurity[83].

The MDR and IVDR impose parallel obligations through their general safety and performance requirements (GSPR)[84], requiring manufacturers to integrate risk management and quality systems into the design phase. For software, this means that already at the design stage, such medical devices should

[75] Art. 43 of the AI Act.
[76] See art. 8 -15 of the AI Act.
[77] Art. 9 of the AI Act.
[78] Art. 10 of the AI Act.
[79] Art. 11 of the AI Act.
[80] Art. 12 of the AI Act.
[81] Art. 13 of the AI Act.
[82] Art. 14 of the AI Act.
[83] Art. 15 of the AI Act.
[84] Annex I, chapter I of the MDR.

ensure repeatability, reliability and performance in line with their intended use[85]. AI based medical devices should be designed with due regard to technical robustness requirements, but also validation of algorithms against representative datasets reflecting clinical populations should be assured.

5.1.1 Risk management system

Both regulatory systems (under AI Act and MDR/IVDR) require the risk management systems to be established, implemented, documented and maintained. Risk management systems should be continuous and iterative, which means that providers of high risk AI systems and manufacturers of the MDs/IVDs must identify known and foreseeable hazards, estimate and evaluate risks, implement control measures and monitor their effectiveness. For software, this includes risks of erroneous outputs, interoperability failures, and cybersecurity vulnerabilities. Annex I MDR/IVDR further mandates that devices achieve a balance between benefits and risks, requiring reduction of risks as far as possible without adversely affecting performance. Usability is a critical element of the risk-management system for AI-enabled medical devices because many risks arise not from the technology itself but from how users interact with it. Effective usability design covering clear outputs, intuitive interfaces, appropriate training, and alignment with the clinical environment, helps ensure that healthcare professionals can correctly interpret and act on AI-generated information. Integrating usability into early design and risk-control measures is essential[86]. Clinical evaluation (MDR) and performance evaluation (IVDR) serve as integral components of this risk management process, ensuring that safety and performance are demonstrated with clinical data. Currently, there is an ISO 14971:2019 norm, recognized as a harmonized standard in support of the MDR[87]. It formulates terminology, principles, and a process for applying risk management to medical devices and is widely referenced by regulators and industry. AI Act specific harmonised standards currently are still under development. In both regulatory regimes, risk management should be treated as an overarching governance architecture. However, whereas the MDR/IVDR focus primarily on clinical and technical safety and performance, the AI Act widens the lens to encompass fundamental rights and socio-technical harms, reflecting its broader normative ambitions.

5.1.2 Data governance and training/validation datasets- The AI Act and the GDPR requirements

AI in medical devices is fundamentally dependent on data. From early development to clinical deployment, training and validation datasets determine not only the accuracy and robustness of AI systems but also their fairness and compliance with fundamental rights. Recognising this, both the AI Act and the GDPR impose obligations on data governance, however from different vantage points. The AI Act addresses technical and ethical risks of biased or inadequate datasets, while the GDPR establishes legal safeguards for the processing of personal and health data. The MDR/ IVDR make general reference to

[85] Annex I, chapter II, point 17 of the MDR.
[86] D.Onitiu, S. Wachter, B. Mittelstadt (n 53).
[87] Recognition of EN ISO 14971 as a harmonized standard in support of the European Medical Device Regulations, <https://committee.iso.org/sites/tc210/home/news/content-left-area/news-and-updates/recognition-of-en-iso-14971-as-a.html> accessed 15 November 2025; Commission Implementing Decision (EU) 2022/757 of 11 May 2022 amending Implementing Decision (EU) 2021/1182 as regards harmonised standards for quality management systems, sterilisation and application of risk management to medical devices [2022] OJ L 138/27.

the EU data protection laws, without introducing the separate data protection mechanisms[88]. It is thus understood that the question of data protection in AI-based medical devices should be governed by the GDPR and AI Act. Together, they create a cumulative framework designed to ensure that healthcare AI systems are trained and validated on data that is both lawful and reliable.

Within the medical devices sector, the AI Act's data-governance regime interacts with, and in important respects intensifies, the data-quality and evidence expectations already embedded in the MDR and IVDR. Under the AI Act, high-risk AI systems, such as machine-learning components integrated into medical or in vitro diagnostic devices, must be developed using training, validation, and testing datasets that meet stringent requirements of relevance, representativeness, completeness, and error control. Providers must implement comprehensive governance practices addressing data provenance, preparation, underlying assumptions, dataset adequacy, and the identification and mitigation of bias, including where necessary the tightly circumscribed processing of special categories of personal data.

The MDR and IVDR, for their part, require that the clinical and performance evidence supporting a device's conformity assessment be grounded in data that are methodologically sound, reliable, and reflective of the device's intended purpose. Clinical and performance evaluations must therefore draw on data generated through well-designed studies and on procedures for verifying, validating, and controlling device design. The resulting documented evidence, including the rationale and outcomes of these verification and validation activities, is subject to scrutiny by notified bodies as part of the conformity assessment process. When read together with the AI Act, this creates a reinforced framework: clinical and performance data must not only meet the established scientific and technical standards of MDR/IVDR but must also satisfy AI-specific data-governance criteria concerning representativeness, bias mitigation, and contextual relevance. As a result, data governance becomes a multi-layered compliance obligation, bridging clinical robustness, model integrity, and the broader socio-technical safeguards introduced by the AI Act.

Article 10 of the AI Act imposes specific obligations on the data used to develop high-risk AI systems. Providers must ensure that training, validation, and testing datasets are relevant, representative, free of errors, and complete, taking into account the system's intended purpose. The aim is to mitigate risks of bias that could undermine safety or result in discriminatory outcomes. In healthcare, where patient data may reflect historical inequalities or underrepresentation of minority populations, this requirement is particularly critical. AI systems trained exclusively on homogeneous datasets may underperform in diverse clinical settings, leading to diagnostic inaccuracies or unequal treatment outcomes.

In addition to representativeness, the AI Act requires that datasets incorporate appropriate statistical properties to minimise risk[89]. Particular focus should be on the intersection between Article 10.5 of the AI Act and Article 9 GDPR. Article 10.5 of the AI Act permits the exceptional processing of special categories of personal data for the narrowly defined purpose of detecting and correcting bias in high-risk AI systems, subject to stringent safeguards and only where no effective alternative, such as anonymised or synthetic data, is available. By contrast, Article 9 GDPR establishes a general prohibition on

[88] art. 110 of the MDR and art. 103 of the IVDR.
[89] Art. 10.3 of the AI Act.

processing such data unless a specific exemption applies, each of which carries its own substantive and procedural conditions. In practice, this dual regime forces manufacturers to demonstrate not only that the use of sensitive data is strictly necessary for bias mitigation under the AI Act, but also that the processing fits within a lawful GDPR derogation. Most commonly it will cover public-interest grounds in the area of public health, or scientific research purposes, each accompanied by appropriate technical and organisational protections. The difficulty is particularly visible in the medical-device context, where the datasets required to develop clinically reliable models often contain health information that is inherently sensitive, and where the representativeness and completeness demanded by both MDR/IVDR evidence standards and Article 10 AI Act cannot be achieved without precisely engaging the categories of personal data most tightly regulated under Article 9 GDPR. This creates a structural tension: the AI Act imposes obligations that may be impossible to fulfil fully without processing sensitive data, yet GDPR allows such processing only under narrowly construed exemptions. Manufacturers therefore face a demanding justificatory burden. They need to show necessity, proportionality, minimisation, and robust safeguards and at the same time ensure that bias-mitigation activities do not inadvertently exceed the permissible boundaries of data processing under EU data-protection law.[90] It should be noted that the abovementioned ambiguities are to be solved by the planned amendment of the GDPR under Digital Omnibus Act. It is not however certain when in which form exactly the change will be introduced[91].

The implementation of the AI Act's data-governance regime will be further shaped by forthcoming horizontal guidance from the European Commission. These guidelines are expected to clarify the practical application of obligations relating to data quality, representativeness, bias assessment, and bias mitigation for high-risk AI systems. In parallel, the Commission's standardisation request has prompted the CEN/CENELEC Joint Technical Committee 21 to develop harmonised standards addressing data management and bias, which will serve as key interpretative and technical references for compliance. For the medical-devices sector, these instruments will play a decisive role in resolving current ambiguities concerning how AI Act requirements interface with MDR/IVDR expectations, particularly in relation to clinical evidence, performance evaluation, and the use of sensitive health data[92].

5.1.3 Technical documentation

Central to lifecycle obligations is the preparation and maintenance of technical documentation, which serves both as a record of compliance and as the basis for conformity assessment. The AI Act introduces a detailed and lifecycle-oriented obligation to prepare and maintain technical documentation for all high-risk AI systems[93]. This documentation must be completed before the system is placed on

[90] See more on these ambiguities, M. van Bekkum, F. Z. Borgesius, 'Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?'(2023) 48 Computer Law & Security Review 5-8; M. van Bekkum, 'Using sensitive data to de-bias AI systems: Article 10(5) of the EU AI act' (2025) 56 Computer Law & Security Review 1-2.
[91] H. Ruschemeier, 'The Omnibus Package of the EU Commission Or How to Kill Data Protection Fast' (17 November 2025) <https://verfassungsblog.de/the-omnibus-package-of-the-eu-commission/> accessed 18 November 2025.
[92] AIB 2025-1 MDCG 2025-6, 12 (n 72).
[93] Art. 11 of the AI Act.

the market or put into service and kept continuously updated. Its core function is evidentiary: it must clearly demonstrate conformity with the high-risk requirements and provide national authorities and notified bodies with sufficiently comprehensive information to assess compliance. Annex IV of the AI Act sets out the minimum required elements, with the aim of assuring transparency, traceability, and demonstrable conformity with high-risk requirements. For medical and in vitro diagnostic devices integrating AI components, this framework operates alongside and must be integrated with the established MDR/IVDR technical documentation regime. Under Annexes II and III MDR/IVDR, manufacturers must maintain technical documentation including device description, design and manufacturing information, safety and performance data, and clinical or performance evaluation reports. A single, consolidated set of technical documentation must encompass both AI-specific elements under the AI Act and device-specific elements required by sectoral legislation. This consolidation avoids duplication but elevates the complexity of compliance, as manufacturers must demonstrate alignment across two regulatory frameworks. In both regimes, the technical file is a "living document," updated throughout the product lifecycle to reflect modifications, new evidence, or corrective measures.

At a minimum, the documentation must include a general description of the AI system (its intended purpose, deployment formats, interfaces, hardware dependencies, versioning, and user instructions), followed by a detailed account of its development process and technical design. This encompasses the system logic and architecture, key design choices and assumptions, data requirements and provenance, human oversight measures, validation and testing methodologies, cybersecurity measures, and, where applicable, pre-determined system changes. The technical file must also capture information on system performance, capabilities and limitations, foreseeable risks, and the appropriateness of performance metrics, as well as a full description of the risk-management system, post-market monitoring arrangements, and the harmonised standards or alternative technical specifications applied[94].

5.1.4 Traceability and record-keeping

Traceability obligations reinforce accountability throughout the supply chain. Article 12 of the AI Act requires providers to keep logs generated by high-risk AI systems and maintain records enabling the reconstruction of system operation during deployment. This complements the MDR/IVDR requirements for unique device identification (UDI)[95], documentation of supply chains, and retention of records for extended periods. For AI systems, traceability also includes documenting training datasets, version histories, and update procedures, ensuring that regulators and healthcare institutions can track changes that may affect system performance.

5.1.5 Transparency and instructions for use

Both frameworks emphasise the importance of clear instructions and labelling, which in the case of the AI Act is linked with the requirement of transparency[96]. Article 13 of the AI Act addresses transparency in a manner distinct from the public-facing identifiability requirement found in Article 50 of the

[94] See annex IV of the AI Act.
[95] See annex VI of the MDR.
[96] Art. 13 of the AI Act.

AI Act. While Article 50 concerns ensuring that individuals can recognise AI-generated content, Article 13 refers to a deeper ethical concern: the opacity of high-risk AI systems and the need for their outputs to remain interpretable by human deployers. As the literature observes[97], Article 13 of the AI Act is structured around two obligations: (1) the intrinsic transparency of the system, and (2) the provision of information to deployers through instructions for use. Although interconnected, these duties differ in nature. The second, concerning providing instructions, is essentially operational and focuses on delivering clear, concise, and accessible information. The first, however, touches on the far more complex question of interpretability and explainability in AI systems. The formulation of Art. 13 of the AI Act, read together with its recital 27 of the preamble exposes a significant weakness. Even if it is stated that high-risk AI systems should be design-transparent enough for deployers to understand their operation, functionality, and limitations, the operative provision achieves transparency primarily through instructions for use. This reflects a superficial approach that does little to engage with the real challenges posed by opaque models in high-stakes domains such as medicine. Article 13 does not mandate the use of interpretable (white-box) models where possible, nor does it require specific XAI techniques where black-box models are deployed. Instead, it places the burden on providers to self-assess and demonstrate compliance upon request, a structure that risks fragmentation and inconsistency in practice.

For medical and in vitro diagnostic devices, where AI systems may inform decisions with direct implications for morbidity or mortality, this regulatory gap is particularly acute. Clinical safety demands not only that outputs be traceable and reliable but also that the underlying mechanisms be sufficiently intelligible to healthcare professionals to enable appropriate scrutiny and intervention. While forthcoming harmonised standards and Commission guidelines on AI transparency may offer greater technical specificity, article 13 itself remains a high-level provision whose prescriptive focus on instructions does not adequately address the interpretability–accuracy trade-offs inherent to advanced AI systems.

As it refers the instructions for use, the MDR/IVDR mandate that devices must be accompanied by instructions for use (IFU) that are comprehensible to the intended user, whether professional or lay-person[98]. The MDR and IVDR impose strict constraints on how medical devices may be labelled, promoted, and presented to users, reflecting the centrality of accurate information to device safety and performance. Devices may not be accompanied by any text, imagery, trademarks, or other signs that could mislead users or patients regarding their intended purpose, clinical function, or risk profile. This includes prohibitions against attributing capabilities the device does not possess, creating unfounded expectations about diagnostic or therapeutic value, omitting information on risks inherent to the intended use, or implying uses outside those forming part of the assessed and authorised intended purpose[99]. These provisions ensure that communication surrounding a device remains tightly aligned with the evidence and conformity assessment underpinning its market authorisation, safeguarding both clinical integrity and patient trust. In healthcare, where AI systems may interact with both clinicians and patients, clarity of instructions is crucial to avoid misinterpretation, overreliance, or improper use.

[97] See more on this, T. Braun, D. E. Harasimiuk, *Legal, Regulatory and Ethical Non-binary Choices of the AI Act* (Routledge 2025) 128.
[98] See, annex I, chapter III, point 23 of the MDR and annex I, chapter III, point 20 of the IVDR.
[99] See art. 7 MDR/IVDR.

The GDPR reinforces the transparency dimension through its articles 12–15, which guarantee data subjects' rights to be informed about how their personal data is processed, for what purposes, and with what consequences. Importantly, Article 22 GDPR establishes safeguards against solely automated decision-making with legal or similarly significant effects, unless subject to explicit consent or necessary for healthcare provision[100]. Patients thus retain a right to meaningful information about the logic involved in algorithmic processing, often described as a "right to explanation."[101]

5.1.6 Human oversight

Human oversight under the AI Act is framed as a core design and operational safeguard, ensuring that high-risk AI systems remain subject to meaningful human control throughout their use[102]. This is particularly the case in the context of AI medical devices. The Act requires that such systems be built with appropriate human–machine interface tools so that oversight can be exercised effectively and in real time. Oversight is directed at preventing or minimising risks to health, safety, and fundamental rights, including risks that remain even after all other requirements for high-risk systems have been applied. This aligns closely with MDR/IVDR obligations to design devices for safe and performant use[103], reinforcing the expectation that AI may support but never displace accountable clinical judgment.

The obligations resulting from the AI Act are risk-sensitive: the degree and form of oversight must correspond to the system's level of autonomy and the context in which it operates. Oversight measures may be embedded directly within the system's design or implemented by deployers, provided these measures have been identified by the provider before market placement. The AI system must also be delivered in a manner that enables assigned human operators to understand its capabilities and limitations, monitor for anomalies, recognise the dangers of automation bias, and correctly interpret its outputs. Crucially, operators must retain the practical ability to disregard, override, or halt the system's functioning through an accessible and safe interruption mechanism.

Both the MDR/IVDR and the AI Act frame human involvement as a condition for protecting individual rights and ensuring informed interaction with AI-enabled devices. MDR/IVDR provisions requiring informed consent in clinical investigations complement the AI Act's broader transparency obligations, which extend beyond research settings to the routine deployment of high-risk AI systems. Together, the requirements on transparency and human oversight ensure that deployers and affected persons receive sufficient information to understand system capabilities, limitations, and risks—and to maintain meaningful human control throughout the AI system's lifecycle[104].

[100] H.B. van Kolfschooten, 'A health-conformant reading of the GDPR's right not to be subject to automated decision-making' (2024) 32 Medical Law Review 373–391, https://doi.org/10.1093/medlaw/fwae029
[101] E. Taylor, 'Explanation and the Right to Explanation' (2024) 10 Journal of the American Philosophical Association 467–482. doi:10.1017/apa.2023.7.
[102] Art. 14 of the AI Act.
[103] Annex I of the MDR/IVDR.
[104] AIB 2025-1 MDCG 2025-6, 16 (n 72).

5.1.7 Accuracy, robustness and cybersecurity

The AI Act introduces obligations to ensure that high-risk AI systems are accurate, robust, and cybersecure throughout their lifecycle. These provisions reflect the EU's commitment to aligning AI with safety and trustworthiness, particularly in healthcare, where algorithmic errors or vulnerabilities may have direct consequences for patient well-being[105]. The regulatory requirements expressed in the AI Act, focus on continuous testing, error resilience, and cybersecurity safeguards.

*Accuracy as a core requirement***.** The AI Act requires high-risk AI systems to achieve levels of accuracy appropriate to their intended purpose and to declare these metrics transparently in accompanying documentation[106]. For healthcare applications, accuracy encompasses diagnostic reliability, predictive validity, and the avoidance of clinically significant false negatives or positives. Developers must specify performance thresholds (e.g., sensitivity and specificity for diagnostic AI), and deployers must monitor whether these thresholds are consistently met in real-world clinical settings. Accuracy is therefore not only a technical specification but also a regulatory benchmark guiding conformity assessments and post-market monitoring.

Robustness and resilience to errors. Robustness refers to an AI system's ability to maintain acceptable performance across varying conditions, inputs, and populations. Systems must be designed to avoid, or at least minimise, errors, inconsistencies, and failures[107]. For healthcare AI, robustness includes ensuring reliable outputs across diverse patient demographics, clinical environments, and data sources. For example, an AI-based radiology tool must perform consistently across imaging equipment from different manufacturers and avoid clinically unacceptable variations in diagnostic outputs. Resilience further requires systems to withstand adversarial perturbations, which are small changes in inputs that could otherwise produce erroneous outputs.

Cybersecurity safeguards. The AI Act explicitly links robustness with cybersecurity[108]. High-risk AI systems must be resilient against attempts to alter their use or performance through malicious attacks. In healthcare, this includes protection against data poisoning (where training datasets are manipulated), adversarial attacks (designed to mislead diagnostic outputs), and system hacking (leading to manipulation of clinical recommendations). Providers must implement security-by-design, regular penetration testing, and incident response mechanisms. Cybersecurity is thus not only an IT concern but a legal obligation under the AI Act, subject to supervisory authority oversight.

Continuous testing and monitoring. The MDR, IVDR, and AI Act collectively embed cybersecurity as a core regulatory obligation throughout the lifecycle of high-risk medical device AI, recognising that device safety and security risks are inseparable. Under the MDR and IVDR, manufacturers must ensure that any risks associated with device operation remain acceptable when measured against the state of

[105] T. Braun, D.E. Harasimiuk, 'AI Deployment in Medical Devices-Ethical and Regulatory Reflections, Beyond Data Protection and Bias – EU perspective' (2023) IEEE Conference on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB), Eindhoven, Netherlands, 2023, 1-6, doi: 10.1109/CIBCB56990.2023.10264892.
[106] Art. 15.1-2 of the AI Act.
[107] Art. 15.4 of the AI Act.
[108] Art. 15.4-5 of the AI Act.

the art, which includes maintaining an appropriate benefit–risk balance across all modes of operation. This necessarily requires an integrated assessment of both "safety" and "security" risks, since cybersecurity failures, such as system manipulation, interference, or data corruption, can directly compromise clinical safety and device performance.

As mentioned above, the AI Act adds further specificity by requiring high-risk AI to incorporate technical solutions that address AI-specific vulnerabilities. Manufacturers must secure AI assets such as training datasets, trained models, and the underlying ICT infrastructure, and they must implement measures to prevent unauthorised access, data or model poisoning, manipulation of outputs, and other cyberattacks[109]. These obligations extend into data governance during system development, requiring secure transmission, storage, and processing of training, validation, and testing data.

Risk assessment plays a central role: manufacturers must systematically identify cybersecurity vulnerabilities and implement mitigation measures proportionate to the risks and the operational context of use. Because cybersecurity is an essential requirement for high-risk AI systems, it forms part of the risk-management system and quality-management system and is subject to conformity assessment under all three regulatory regimes.

5.2 Obligations of manufacturers and providers

The obligations imposed on providers of high-risk AI systems under the AI Act and the obligations of medical-device manufacturers under the MDR/IVDR form two parallel, yet interdependent, compliance frameworks. Their intersection becomes particularly important for AI-enabled medical devices which must simultaneously satisfy the AI Act's horizontal requirements discussed above and the MDR/IVDR's sector-specific obligations.

Under the AI Act, providers of high-risk AI systems must:

- ensure full compliance with the substantive requirements of Chapter III Section 2 of the AI Act, which were analysed in point 4.1 above,
- establish a quality management system,
- maintain extensive technical documentation,
- retain system logs,
- undergo conformity assessment,
- draw up the EU declaration of conformity,
- affix the CE marking, and
- implement corrective actions when non-compliance is detected,
- register their systems in the EU database established under art. 49 of the AI Act,
- respond to competent-authority requests and show the conformity with chapter III sect. 2 requirements, and
- ensure accessibility in line with EU accessibility law.

The AI Act's obligations are lifecycle-oriented and aim to guarantee that high-risk AI systems are safe, transparent, technically robust and traceable from design to post-market operation[110].

[109] AIB 2025-1 MDCG 2025-6, 16-19 (n 72).
[110] Art. 16 of the AI Act.

Manufacturers of medical devices face an equivalent, though more clinically structured, set of responsibilities under the MDR and IVDR[111]. They must:

- design and manufacture devices in conformity with general safety and performance requirements,
- maintain a risk-management system,
- conduct a clinical or performance evaluation,
- prepare and update detailed technical documentation,
- operate a comprehensive quality-management system covering design, production, post-market surveillance, vigilance, supplier controls, and continuous improvement,
- affix the CE marking,
- register devices,
- retain documentation for 10–15 years,
- ensure availability of information in appropriate languages,
- undertake corrective actions, and
- cooperate fully with competent authorities.

For manufacturers of MDAI, these two regimes converge into a compound regulatory architecture. AI components embedded in a medical device trigger the AI Act's provider obligations, while the device as a whole remains subject to the MDR/IVDR. In practice, this means:

- Dual regimes for conformity assessment: the AI system integrated in the medical device (or being device itself) must fulfil AI Act requirements (e.g. data governance, transparency, human oversight, cybersecurity), while the overall device must meet MDR/IVDR safety and performance requirements. A single technical file may be used, but it must simultaneously satisfy Annex IV of the AI Act and Annexes II–III of the MDR/IVDR.
- Integrated quality and risk-management systems: manufacturers must align AI-specific risk-management measures with the MDR/IVDR risk-management system. It shall ensure consistency across clinical, technical, and algorithmic risks. Similarly, the AI Act's QMS requirements must be embedded within the broader MDR/IVDR quality system. Risk management and quality management systems (QMS) represent the backbone of lifecycle regulation for AI in healthcare. Both the MDR/IVDR and the AI Act impose comprehensive obligations on developers and providers, reflecting a preventive regulatory philosophy: risks must be systematically identified, mitigated, and monitored, rather than merely corrected once they materialise. While their conceptual foundations are aligned, the frameworks differ in scope, focus, and operational detail. The QMS under MDR/IVDR is subject to the European harmonised standard EN ISO 13485:2016 - Medical devices – Quality management systems – Requirements for regulatory purposes[112]. The MDR/IVDR QMS should integrate clinical evaluation, where a risk-benefit ratio analysis is one of the foundational concepts.
- Continuous post-market obligations: both frameworks require ongoing monitoring, logging, vigilance, security updates, and corrective actions. For MDAI, this results in a heightened expectation that post-market surveillance captures both clinical performance and AI-specific risks such as drift, error propagation, and data/model poisoning.
- Regulatory accountability: roles of AI Act's providers and MDR/IVDR's manufacturers coincide for MDAI. This means that the same economic operator must ensure compliance with both

[111] Art. 10 of the MDR/IVDR.
[112] Commission Implementing Decision (EU) 2022/757 (n 87).

regulatory regimes, respond to competent-authority requests, and maintain extensive documentation for auditability. The combined effect is a comprehensive, multilayered framework designed to ensure not only the clinical safety and performance of the medical device, but also the technical robustness, transparency, data governance integrity, cybersecurity, and human oversight demanded by AI regulation.

5.3 Liability regime regarding AI Medical Devices

5.3.1 Revised PLD and its implications for AI Medical Devices

The governance of AI in healthcare cannot be reduced to ex ante regulatory compliance alone[113]. Effective protection also requires robust ex post mechanisms to ensure compensation when harms occur. In the EU legal order, liability rules intersect with regulatory frameworks such as the MDR, IVDR, AI Act, and GDPR, each of which contributes to shaping responsibility for defective products, malfunctioning AI systems, or unlawful data processing.

Within the regulatory architecture governing AI medical devices, neither the AI Act nor the MDR/IVDR introduces technology-specific liability rules. Instead, manufacturers and other economic operators remain subject to general, technology-neutral liability regimes established by the revised Product Liability Directive (PLD)[114], complemented by national tort and contract law. The revised PLD significantly recalibrates the liability mechanisms for AI medical devices. One of the most important shifts in the revised PLD lies in its explicit inclusion of software as both a "product" and a "component," thereby capturing standalone AI systems, embedded MDAI modules, and continuous-learning software updates within the scope of product liability. Liability now extends beyond manufacturers to importers, distributors, authorised representatives, and parties undertaking substantial modifications outside the manufacturer's control[115].

The PLD establishes two independent bases for determining defectiveness:

1. whether the product fails to provide the level of safety a person is entitled to expect; and
2. whether it fails to meet safety requirements imposed by EU or national law.

The second basis creates a direct normative bridge to the MDR and the AI Act. Requirements relating to general safety and performance requirements, risk management, transparency, human oversight, cybersecurity, data governance, and post-market monitoring can all function as "safety requirements."

[113] G. Malgieri and F. Pasquale, 'Licensing High-Risk Artificial Intelligence: Toward Ex Ante Justification for a Disruptive Technology' (2024) 52 Computer Law & Security Review 105899.
[114] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC [2024] OJ L 2024/2853.
[115] A. Parziale, 'AI-powered Medical Devices and the Development Risk Defense Under the Revised Product Liability Directive' in: F. Casarosa, F. Gennari, A. Rossi, (eds) *Enabling and Safeguarding Personalized Medicine,* Data Science, Machine Intelligence, and Law (vol. 7 2025 Springer, Cham) 285. https://doi.org/10.1007/978-3-031-99709-9_14

Thus, a breach of obligations under the MDR or the AI Act may not only lead to regulatory non-compliance but may also independently constitute evidence of defectiveness under the revised PLD.

Recognising that AI medical devices often evolve through updates, retraining cycles, or continuous learning, the revised PLD emphasises ongoing monitoring duties across the entire lifecycle of the device, potentially up to 25 years. This is reinforced by provisions addressing adaptive technologies, software updates, and residual obligations even after devices are placed on the market. Importantly, a manufacturer cannot rely on the traditional "development risk defence"[116] if a software update could have prevented the harm[117].

The revised PLD expands a notion of damage to include verified psychological injury and data loss, both of which are pertinent in the context of medical devices, where misuse, erroneous outputs, or cybersecurity breaches may directly compromise sensitive health data. Liability thresholds have been abolished, the limitation period extended, and options for exculpation narrowed, especially for software manufacturers who fail to provide necessary updates that could have prevented the defect[118].

The revised PLD also introduces procedural mechanisms that significantly lower the claimant's evidentiary burden. If a claimant establishes the plausibility of a defect, the defendant must disclose relevant evidence, with failure to do so creating a presumption of defectiveness. This may create friction with confidentiality obligations and challenges in contexts where AI opacity makes causal mechanisms difficult to trace. In certain cases, courts may be obliged to presume causation where the nature of the technology, especially adaptive or opaque AI, makes proof particularly onerous. The recitals explicitly acknowledge AI and medical devices, signalling that the legislator intended these presumptions to facilitate claims involving complex automated systems[119].

The withdrawal of the proposed AI Liability Directive (AILD) in early 2025 signals a policy choice to regulate AI liability through the revised PLD and national private-law systems, rather than through a dedicated, technology-specific liability regime[120]. While this reduces legislative fragmentation, it heightens the importance of cross-regulatory interpretation. Critically, compliance with the MDR and the AI Act does not create a safe harbour under the PLD; conformity assessment and CE marking do not shield manufacturers from liability if a defect can be established under the revised standards. For manufacturers of AI-enabled medical devices, this results in a substantially strengthened liability environment, where regulatory non-compliance and failure to manage software-related risks can readily translate into civil liability exposure.

[116] C. Newdick, 'The Development Risk Defence of the Consumer Protection Act 1987' (1988) 47 The Cambridge Law Journal 455–476. doi:10.1017/S0008197300120458.
[117] See art. 11.2 b) of the revised PLD Directive.
[118] B. Schütte, ' Product Liability in the Future framework of AI (Technology) Regulation' in:
M Bergström & V Mitsilegas (eds), *EU law in the digital age*, Swedish Studies in European Law (vol. 19 2025 Hart publishing) 92 https://doi.org/10.5040/9781509981212.ch-00692
[119] See recital 48 of the revised PLD Directive.
[120] L. Nannini, 'When Less Regulation Means More Complexity: The EU AI Liability Directive Withdrawal and Its Impact on European Technological Competitiveness' (2025) 8 Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society 1848-61, doi:10.1609/aies.v8i2.36679.

5.3.2 The GDPR compensation rights

The GDPR introduces an autonomous liability mechanism focused on compensation for data protection breaches. Article 82 GDPR establishes a right for any person who has suffered material or non-material damage as a result of an infringement to receive compensation from the controller or processor. The regime is broad: controllers and processors may be held jointly and severally liable, unless they prove they are not responsible for the damage. For AI in healthcare, where breaches of sensitive health or genetic data can cause significant psychological, reputational, or economic harm, this right provides a powerful enforcement tool. Financial consequences include not only compensation but also potential administrative fines of up to 20 million EUR or 4% of annual global turnover[121].

5.3.3 Interplay and cumulative protection

The combination of MDR/IVDR, AI Act, revised PLD and GDPR ensures that liability in healthcare AI is not confined to a single legal axis. Patients harmed by defective AI-based devices can claim under product liability rules; those whose rights are infringed through unlawful data processing can seek compensation under GDPR.

Financial coverage requirements embedded in MDR/IVDR such as liability insurance[122] (Article 10.16 of the MDR/IVDR), ensure that manufacturers are in a position to compensate patients and healthcare institutions in the event of harm, together with the growing emphasis on insurance mechanisms for AI systems, ensure that these rights are not merely theoretical. Developers and providers must therefore anticipate liability risks and integrate insurance, contractual risk allocation, and compliance strategies into their business models. For healthcare institutions, clarity on liability allocation is essential to safeguard both patients' rights and institutional sustainability.

6 Obligations of Deployers and Users of AI Medical Devices

6.1 Deployment and use of AI in medical devices sector

The AI Act distinguishes clearly between the obligations of the provider and the deployer. This division is particularly important in healthcare, where hospitals, clinics, and laboratories typically act as deployers rather than providers. While providers bear the primary responsibility for lifecycle compliance, deployers carry distinct obligations that ensure AI systems are applied safely, transparently, and in accordance with their intended purpose.

The AI Act introduces a detailed framework of responsibilities for deployers of high-risk AI systems, mirroring and expanding the long-standing obligations placed on professional users of medical devices under the MDR and IVDR. While the MDR/IVDR focus on ensuring safe, appropriate, and informed use of medical technologies in clinical environments, the AI Act adds AI-specific governance duties that reflect the distinct risks associated with automated decision systems.

[121] Art. 83 of the GDPR.
[122] Art. 10.16 of the MDR and art. 10.15 of the IVDR.

Under the AI Act, deployers of high-risk AI systems must use the system strictly in accordance with the provider's instructions, taking appropriate technical and organisational measures to ensure safe and compliant operation[123]. This obligation echoes the MDR/IVDR expectation that professional users handle devices in line with the manufacturer's intended purpose, training requirements, and safety information. MDR and IVDR oblige manufacturers to provide users with clear instructions for safe use[124]. Users, in turn, are expected to operate devices in accordance with these instructions and with professional standards of care. Although the regulations do not establish direct legal penalties for end-users, their correct use of devices is integral to manufacturers' post-market surveillance systems, which depend on feedback from healthcare professionals. For AI medical devices, this creates a dual compliance expectation: clinicians and healthcare institutions must respect both device-level operating requirements and AI-specific safeguards.

A central obligation for deployers under the AI Act is the assignment of competent human oversight[125]. The AI Act requires that oversight be entrusted to individuals with adequate training, authority, and support, ensuring that human decision-makers retain meaningful control. This aligns with MDR/IVDR principles of clinical responsibility, under which professional users remain accountable for medical decisions and must understand the capabilities and limits of the device. In the medical devices AI context, oversight thus becomes both a safety requirement and a risk-mitigation measure. Healthcare professionals must monitor AI outputs, detect anomalies, and be prepared to disregard or override the system when needed.

Where deployers have control over input data, the AI Act obliges them to ensure its relevance and representativeness[126]. It is supposed to mitigate the risk when improper inputs can compromise device performance and overall patient safety.

The AI Act goes further by imposing post-market responsibilities on deployers. They must monitor the operation of the system, retain logs under their control, and report serious incidents or emerging risks to the provider and competent authorities[127]. This obligation mirrors the vigilance duties of professional users under MDR/IVDR, who must report adverse events, participate in corrective actions, and contribute to post-market surveillance. MDR[128] and IVDR[129] require vigilance systems to capture and analyse incidents. Healthcare professionals are often the first to detect anomalies in AI performance, making their feedback crucial to manufacturers' ability to implement corrective actions or recalls.

Overall, the AI Act and the MDR/IVDR establish a complementary set of expectations for those using AI-enabled medical devices: professional users must combine safe clinical use with AI-specific operational vigilance, robust oversight, and responsible data practices. In this dual framework, deployers become essential actors in maintaining the safety, reliability, and ethical operation of high-risk MDAI

[123] Art. 26. 1 of the AI Act.
[124] Art. 10.11 of the MDR.
[125] Art. 26.2 of the AI Act.
[126] Art. 26.4 of the AI Act.
[127] Art. 26.5-6 of the AI Act.
[128] Art. 87-92 of the AI Act.
[129] Art. 82-86 of the AI Act.

throughout its lifecycle. For healthcare institutions, these duties translate into both legal and organisational responsibilities. Hospitals deploying AI-based diagnostic software must implement internal governance mechanisms ensuring staff are trained[130], logs are retained, and feedback loops with providers are functional. Failure to meet deployer obligations may expose institutions to liability, particularly where patient harm results from misuse or insufficient oversight.

6.2 Fundamental Rights Impact Assessment – implications for the healthcare sector

The introduction of the Fundamental Rights Impact Assessment (FRIA)[131] under the AI Act adds a new layer of governance that has no direct analogue in the MDR or IVDR. FRIA targets deployers who are bodies governed by public law or are private entities providing public services. Those entities are obliged to perform an assessment of the impact on fundamental rights that the use of a given high-risk AI system may produce. It has important implications for the deployment of AI-enabled medical devices, particularly in settings where public bodies or providers of public services use high-risk MDAI. The FRIA introduces a complementary perspective centred on fundamental rights, including autonomy, non-discrimination, privacy, dignity, and access to health services[132].

Under Article 27 AI Act, certain deployers, such as public hospitals, publicly funded healthcare networks, and private providers delivering public services, must carry out a FRIA before putting a high-risk AI system into use. This assessment requires deployers to analyse how the system will fit into their clinical processes, which groups of patients might be affected, what specific risks of harm may arise, and how human oversight will be implemented. The FRIA must also document governance measures and complaint mechanisms, ensuring that affected persons have channels to contest decisions influenced by the AI system[133].

Although the FRIA is not a requirement of the MDR/IVDR, it resonates with several of their underlying principles. Medical-device law already emphasises respect for patient rights through requirements for informed consent in clinical investigations, transparency about device risks, and vigilance mechanisms that ensure patients' safety post-market. The FRIA adds to this a set of obligations addressed to deployers to reflect on issues such as potential discrimination against vulnerable patient groups, unequal access to care, opacity of algorithmic decision-making, or the risk that automation might distort the clinician–patient relationship.

In practical terms, integrating a FRIA into the deployment of AI medical devices means that healthcare institutions must decide whether its use may inadvertently generate rights-based harms, such as biased diagnostic, reduced patient autonomy, disproportionate impacts on certain groups, or insufficient

[130] AIB 2025-1 MDCG 2025-6, 26-27 (n 72).
[131] Art. 27 of the AI Act.
[132] A. Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template' (2024) 54 Computer Law & Security Review 106020 https://doi.org/10.1016/j.clsr.2024.106020
[133] Art. 27.1 of the AI Act.

human oversight. Because the FRIA must take into account the information provided by the manufacturer under Article 13 AI Act, it also creates an operational dependence between the provider's transparency obligations and the deployer's ability to assess rights implications.

Ultimately, the FRIA extends the concept of "benefit–risk" beyond clinical outcomes. It requires healthcare deployers to examine the technology's interaction with human rights and ethical values, ensuring that the introduction of high-risk AI medical devices into medical practice is aligned not only with medical-device regulation but also with the EU's fundamental-rights framework.

6.3 In-house manufacturing and exemptions under the MDR/IVDR

Hospitals, clinics, and laboratories increasingly act not merely as passive users but as active participants in developing or adapting medical software. Article 5.5 of the MDR/IVDR provides an exemption for health institutions that manufacture, modify, or use devices internally without placing them on the market. Such "in-house" devices need to comply with GSPR, but are exempt from many of the manufacturer obligations, including CE marking and conformity assessment, provided that specific conditions are met:

- The devices are manufactured and used solely within health institutions.
- They are not transferred to another legal entity.
- Their manufacture and use take place under an appropriate quality management system.
- The health institution justifies that the patient group's specific needs cannot be met by an equivalent CE-marked device on the market.
- Documentation on manufacturing, design, and performance and intended purpose is drawn up and made available to competent authorities.
- The institution must ensure that manufacturing follows the documentation and continuously review clinical experience, implementing corrective actions where necessary.
- The institution must supply information to its competent authority on request, publish a declaration identifying the device and confirming compliance with the GSPR (or explaining any justified deviations)

In-house AI medical devices will also escape AI Act's high-risk requirements. It is due to the fact that AI systems are considered high-risk under the AI Act only if, among other conditions, the corresponding medical device or in vitro diagnostic device is subject to a third-party conformity assessment carried out by a notified body under the MDR or IVDR. This means that in-house medical devices and IVDs, those developed and used exclusively within health institutions in the Union, do not fall under this criterion[134].

[134] K. Kalodanis et al., 'Evaluating the Impact of the EU AI Act on Medical Device Regulation' in John Mantas et al. (eds), Envisioning the Future of Health Informatics and Digital Health (IOS Press 2025) 41.

Accordingly, in-house AI medical devices do not qualify as a high-risk AI system under Article 6.1 of the AI Act. However, this exemption is limited: such systems remain subject to other AI Act obligations, including compliance with prohibited AI practices and any applicable general requirements[135].

7 Data Protection and Governance

7.1 GDPR principles applied to health and AI data

The GDPR establishes a principled framework for the lawful processing of personal data. As was discussed above, health data, together with genetic and biometric data, falls within special categories of personal data under Article 9 GDPR, enjoying enhanced protection due to its sensitivity. AI systems, in turn, frequently rely on the large-scale collection and analysis of such data, both for development and deployment. Applying GDPR principles in this context ensures that innovation in digital health remains aligned with the fundamental rights of patients.

The core data-protection principles set out in Article 5 GDPR act as a baseline for lawful and trustworthy data use and must be integrated into both the technical design of the AI system and the organisational practices of the provider/manufacturer and user/deployer.

AI medical devices must ensure lawfulness, fairness and transparency[136], meaning that any processing of personal data, including training data, real-world inputs, or post-market monitoring data, must have a valid legal basis, be understandable to patients and users, and avoid hidden or unexpected uses. The cornerstone of GDPR compliance is that processing must have a valid legal basis[137] and, for special categories, meet one of the exceptions clearly indicated in the regulation[138]. In healthcare, the most relevant bases are the provision of medical diagnosis and treatment[139] and processing for scientific research in the public interest, subject to safeguards[140]. For AI developers, lawfulness requires a clear articulation of why patient data is processed, whether in clinical deployment or for training and validation of models. Without such a basis, processing remains unlawful regardless of potential medical benefits.

Fairness requires that data subjects are not misled or subjected to unjustified outcomes. In AI healthcare, fairness extends beyond individual consent to structural issues such as bias in datasets. For example, if training datasets underrepresent certain demographic groups, AI systems may produce systematically less accurate diagnoses for those populations. Such outcomes may breach both the fairness principle and anti-discrimination norms. Controllers must therefore design processes that actively mitigate bias and ensure equitable treatment across patient groups.

Transparency entails that patients are informed, in clear and accessible terms, about how their data is used, for what purposes, and with what consequences. Under Articles 12–14 GDPR, this includes

[135] AIB 2025-1 MDCG 2025-6, 26 (n 72).
[136] Art. 5.1 a), and art. 6 of the GDPR.
[137] Art. 6 of the GDPR.
[138] Art. 9.2 of the GDPR.
[139] Art. 9.2 h) of the GDPR.
[140] Art. 9. 2 j) of the GDPR.

providing information on the existence of automated decision-making, including meaningful information about the logic involved. In AI contexts, the challenge lies in conveying complex algorithmic processes to patients without overwhelming them. Transparency also underpins trust: patients who understand how AI supports their care are more likely to accept its integration into clinical practice.

Purpose limitation requires that data be collected only for clearly specified clinical or operational purposes and not repurposed in ways incompatible with those aims unless research or public-interest exemptions apply[141]. The purpose limitation plays crucial role in legitimizing data processing and serves as the reference point for assessing its necessity, appropriateness, completeness and duration[142]. This is particularly relevant for AI, which often operates in iterative cycles where data collected for one purpose may be repurposed for model improvement. The GDPR purpose limitation principle may restrict secondary use of clinical data for AI training unless compatible with the original purpose or justified under research exemptions, potentially conflicting with iterative AI development practices. Secondary use of personal data is subject to a strict compatibility framework under the GDPR. It is particularly relevant for AI-enabled medical devices that often depend on re-using clinical or operational data for training, improvement, validation, or post-market monitoring. When the intended secondary purpose is incompatible with the original purpose of collection, the data may not be reused unless a new legal basis applies. Typically, explicit consent is needed or there is a specific legal framework that authorises such processing for important public-interest objectives, such as public health or medical research[143]. Without such a basis, secondary use is prohibited. If the secondary use is compatible with the initial purpose, the controller may rely on the same legal basis used for the original processing. Controllers must inform data subjects about the further processing and their rights, ensure compliance with data-minimisation and security requirements, and carry out a data-protection impact assessment where necessary. The outcome of the compatibility assessment, along with any measures taken to safeguard data subjects, must be fully documented to satisfy the GDPR's accountability principle. In the context of AI medical devices, this means that secondary use, whether for model retraining, performance enhancement, bias monitoring, or safety analytics, must always be justified, transparent, and grounded in a defensible legal basis.

Given that AI models rely heavily on large datasets, the principle of data minimisation is particularly relevant[144]. Only the data strictly necessary for the device's functioning and safety may be processed. Developers and healthcare institutions must ensure that data used for training or deployment is proportionate and targeted, and that superfluous or redundant attributes are excluded. Techniques such as pseudonymisation, anonymisation, and federated learning can help reconcile the need for data-

[141] Art. 5.1 b) of the GDPR.

[142] R. Mühlhoff, H. Ruschemeier, 'Updating purpose limitation for AI: a normative approach from law and philosophy' (2025) 33 International Journal of Law and Information Technologies 6-7.

[143] J. Meszaros, M. C. Compagnucci, and T. Minssen, 'The Interaction of the Medical Device Regulation and the GDPR: Do European Rules on Privacy and Scientific Research Impair the Safety and Performance of AI Medical Devices?', in I.G. Cohen et al. (eds.) *The Future of Medical Device Regulation: Innovation and Protection* (2022) Cambridge University Press, 80-82.

[144] Art. 5.1 c) of the GDPR.

intensive AI with minimisation requirements. The principles of accuracy[145] and storage limitation[146] are linked to the problem that poor-quality or outdated data can directly undermine the safety and performance of AI systems, while unnecessary retention of identifiable patient information increases privacy risks. Finally, integrity and confidentiality require robust technical and organisational safeguards to protect data from unauthorised access, loss, manipulation, or cybersecurity incidents[147]. These issues are particularly acute for AI systems vulnerable to data poisoning or model-manipulation attacks. The AI Act's requirement for representative datasets may demand broader or more diverse data collection than strictly necessary under GDPR's minimisation principle. Balancing sufficiency for robustness with limits on excess collection is a practical challenge.

Overlaying all these principles is the requirement of accountability: controllers, who in the context of AI medical devices may be manufacturers, providers, deployers, healthcare institutions as professional users, must be able to demonstrate compliance, not merely claim it. For AI medical devices, this means embedding GDPR principles into system design, documentation, and lifecycle management, ensuring that data protection is treated as a continuous obligation aligned with both MDR/IVDR and AI Act, especially since most of GDPR principles correspond to AI Act's high-risk AI systems' requirements.

7.2 MDR/IVDR requirements for clinical and performance data integrity

The MDR and the IVDR embed a data-centric approach to safety and performance. Unlike the AI Act, which addresses the quality of training and validation datasets in algorithmic development, MDR and IVDR focus on the integrity of clinical and performance data underpinning device evaluation and market approval. These data requirements are critical for ensuring that medical devices, including AI-based software and in vitro diagnostic systems, demonstrate not only technical functionality but also clinical benefit and reliability in real-world conditions.

7.2.1 Clinical evaluation under MDR.

The MDR establishes clinical evaluation as a central pillar of the conformity assessment process, reflecting the principle that safety and performance must be demonstrated through evidence, not presumed[148]. For medical devices, including AI-based software with diagnostic or therapeutic purposes, clinical evaluation ensures that products are not only technically functional but also deliver tangible clinical benefit to patients under real-world conditions.

Every medical device, regardless of class, must undergo an evaluation unless explicitly exempted (e.g., certain Class I devices). For AI-enabled software, Rule 11 of Annex VIII generally places such systems in Class IIa or higher, making rigorous clinical evaluation an essential component of market approval.

[145] Art. 5.1 d) of the GDPR.
[146] Art. 5.1 e) of the GDPR.
[147] Art. 5.1 f) of the GDPR.
[148] Art. 61-62 and annex XIV of the MDR.

Specifically, manufacturers, through clinical evaluation process, while demonstrating conformity with GSPRs must establish:

- Safety: that the device does not pose unacceptable risks when used as intended.
- Clinical benefit: that the device achieves its intended medical purpose, such as improving diagnosis, monitoring, or treatment outcomes.
- Favourable benefit–risk ratio: that benefits outweigh residual risks, taking into account available alternatives.

For AI systems, this translates into demonstrating that algorithmic outputs are accurate, clinically meaningful, and do not generate unacceptable risks (e.g., false negatives in cancer detection). The process of clinical evaluation involves a systematic and critical assessment of clinical data pertaining to the device. Clinical data may be drawn from[149]:

- Clinical investigations conducted on the device itself.
- Clinical investigations or other scientific studies involving an equivalent device, where equivalence can be demonstrated.
- Peer-reviewed publications describing clinical experience with the device or with an equivalent device.
- Clinically relevant findings emerging from post-market surveillance activities, including post-market clinical follow-up.

The evaluation must demonstrate conformity with the GSPRs set out in Annex I of the MDR, particularly that the device achieves its intended purpose without compromising patient health or safety. For AI-enabled devices, this means that algorithmic outputs must be validated against robust clinical evidence demonstrating their reliability and utility in diagnostic or therapeutic contexts.

For the purpose of conducting clinical investigation, there is an international standard EN ISO14155:2020 Clinical investigation of medical devices for human subjects - Good clinical practice, which addresses good clinical practice for the design, conduct, recording and reporting of clinical investigations[150]. It outlines the clinical investigation plan which sets out the rationale, objectives, design methodology, monitoring, conduct, record-keeping, and the method of analysis for the clinical investigation[151]. Manufacturers must compile their findings into a clinical evaluation report, which integrates scientific validity, analytical performance, and clinical performance data[152].

[149] Art. 2 point 48 of the MDR.
[150] Commission Implementing Decision (EU) 2021/611 of 14 April 2021 amending Implementing Decision (EU) 2020/438 as regards harmonised standards on biological evaluation of medical devices, packaging for terminally sterilised medical devices, sterilisation of health care products and clinical investigation of medical devices for human subjects [2021] OJ L129/158.
[151] MDCG 2024-3, Guidance on content of the Clinical Investigation Plan for clinical investigations of medical devices (March 2024) 6.
[152] Art. 61.12 of the MDR.

7.2.2 Performance evaluation under IVDR.

The IVDR establishes a rigorous framework for performance evaluation, reflecting the particular sensitivity of diagnostic information in clinical decision-making[153]. While the MDR requires clinical evaluation for medical devices, the IVDR imposes performance evaluation obligations tailored to the diagnostic context. The regulation conceptualises performance evaluation as an integrated and continuous process throughout the lifecycle of a device. The process is designed to demonstrate that the device achieves the intended purpose, supports safe and effective use, and conforms to the GSPRs listed in Annex I of the IVDR.

Performance evaluation comprises three interrelated elements:

1. Scientific validity: refers to the demonstration of the association between the analyte (e.g., a biomarker, genetic variant, or molecular marker) and the clinical condition or physiological state of interest. Scientific validity provides the foundational rationale for why the test matters in clinical practice.

2. Analytical performance: concerns the ability of the device to correctly detect or measure the analyte. Metrics include sensitivity, specificity, accuracy, repeatability, reproducibility, and limits of detection. In AI contexts, analytical performance translates into the reliability of algorithms when processing laboratory or imaging data. It needs to be demonstrated that the software consistently and accurately interprets inputs, even across diverse laboratory environments and equipment settings.

3. Clinical performance: assesses the ability of the device to produce results correlated with the target clinical condition, thereby enabling meaningful medical decisions. Evidence is generated through clinical performance studies[154], which are subject to ethical review, informed consent requirements, and rigorous methodological design. For AI-based diagnostics, this may mean demonstrating that the algorithm's predictions correlate strongly with physician-confirmed diagnoses, or that the tool improves patient management by enabling earlier detection of disease[155].

Manufacturers must generate a performance evaluation report (PER), regularly updated throughout the device lifecycle, which serves as the cornerstone for conformity assessment. For AI-enabled diagnostic software, this may involve demonstrating that the algorithm consistently interprets given data with clinically acceptable accuracy across diverse populations.

7.2.3 Data integrity requirements.

Both MDR and IVDR underscore that the clinical and performance data underpinning evaluations must be robust, reliable, and generated according to recognised scientific and ethical standards[156] Annex XV

[153] Art. 56–58 and Annex XIII of the IVDR.
[154] Annex III, part A of the IVDR.
[155] N. Tomašev et al., 'Use of Deep Learning to Develop Continuous-Risk Models for Adverse Event Prediction from Electronic Health Records' (2021) 16(6) Nature Protocols 2785.
[156] Art. 62.3 of the MDR.

MDR and Annex XIII IVDR detail requirements for clinical investigations and performance studies, including protocols, ethical review, data monitoring, and statistical methods. Complying with ethical standards should be confirmed by the statement in clinical investigation plan specifying that the clinical investigation shall be conducted in accordance with the ethical principles that have their origin in the Declaration of Helsinki[157].

For AI-based devices, the abovementioned requirements intersect with algorithmic concerns: dataset representativeness, reproducibility of validation studies, and monitoring for performance drift over time. Consequently, data integrity encompasses:

- Completeness: sufficient sample sizes and population diversity to ensure generalisability.
- Reliability: validated study designs and appropriate controls to minimise bias.
- Traceability: documentation of study conduct, data provenance, and analysis.

In the case when clinical and performance data are at stake, the processing of patient-level data is a particularly sensitive topic. Here, GDPR safeguards apply in parallel: informed consent may be required for participation in studies; data minimisation principles govern the scope of collection; and pseudonymisation or anonymisation techniques are recommended to mitigate risks. Regulators and notified bodies reviewing MDR/IVDR submissions will rely on GDPR compliance to validate the legitimacy of data used in device evaluation.

7.2.4 Post-market data and continuous evaluation.

The MDR[158] and IVDR[159] extend data integrity requirements beyond pre-market assessment by mandating Post-Market Surveillance (PMS) and, for higher-risk devices, periodic safety update reports (PSURs). These mechanisms ensure that performance is continuously assessed in real-world practice. In the AI context, PMS is essential to detect issues such as declining accuracy due to evolving patient populations, or software updates altering system behaviour.

Important elements of PMS are Post-Market Clinical Follow-up (PMCF) for medical devices and Post-Market Performance Follow-up (PMPF) for in vitro diagnostic devices. Under the MDR and IVDR, PMCF and PMPF are continuous, proactive processes embedded in the manufacturer's PMS plan and intended to update the clinical or performance evaluation throughout the device's lifetime. For AI-enabled devices these are essential for maintaining algorithmic data integrity, a prerequisite for sustained safety, performance, and clinical benefit.

[157] MDCG 2024-3 (n 151) 17; WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Participants, Adopted by the 18th WMA General Assembly, Helsinki, Finland, June 1964, https://www.wma.net/policies-post/wma-declaration-of-helsinki/ access 20 November 2025.
[158] Art. 83-86 of the MDR.
[159] Art. 78-81 of the MDR.

A PMCF plan must specify the methods for gathering clinical data on the real-world use of the CE-marked device within its intended purpose. In traditional devices, this serves to confirm long-term safety, detect new side effects, monitor emergent risks, and verify the continued acceptability of the benefit–risk profile. In the context of AI systems, PMCF must do all of this and more[160]. It must ensure that the data flowing into the system in clinical practice remain representative, accurate, and aligned with the assumptions under which the algorithm was developed and validated[161]. This is because AI models are vulnerable to data drift, demographic shifts, changes in clinical workflows, and variations in measurement practices. If the real-world data begin to diverge from the training or validation datasets, the algorithm's outputs may degrade, lose calibration, or develop performance disparities across subpopulations. PMCF therefore becomes the primary mechanism for detecting such phenomena early, allowing manufacturers to analyse algorithmic performance against clinical endpoints and to identify patterns suggesting bias, instability, or unexpected behaviour.

Similarly, PMPF, the IVDR counterpart, serves the same structural function for in vitro diagnostic devices. It focuses on performance characteristics, such as analytical sensitivity and specificity, precision, diagnostic accuracy, and potential interferences. PMPF ensures that real-world laboratory use does not introduce deviations that could compromise diagnostic reliability. Like PMCF, PMPF findings must be analysed, reported, and integrated into the device's ongoing performance evaluation[162].

7.2.5 Integrating of the AI Act requirements into clinical and performance evaluations

MDR and IVDR requirements ensure that medical devices, including AI-driven tools, are grounded in evidence-based medicine. Clinical and performance evaluations are not a one-off task but a lifecycle obligation, reinforced through PMS and vigilance systems. For developers of healthcare AI, compliance requires more than technical validation of algorithms; it demands rigorous demonstration of clinical benefit, supported by robust, reliable, and ethically generated data. The intersection of the AI Act with the MDR and IVDR becomes particularly significant in the generation of clinical evidence, especially when high-risk AI systems qualify as medical devices or in vitro diagnostic devices. The AI Act introduces additional, AI-specific obligations that must be integrated into the design and conduct of clinical investigations and performance studies.

Regulatory duties under MDR and IVDR result in the studies, which must generate robust, methodologically sound data demonstrating that the AI medical devices perform as intended in the target patient population. Evaluations must include software verification and validation, clinical validation of outputs, and the generation of sufficient clinical evidence to support claims of safety and clinical benefit. For AI-based devices, this involves assessing performance metrics such as accuracy, precision, analytical validity, clinical validity, and usability.

[160] R. Kilian, L. Jäck, D. Ebel (n 60) 1-25.
[161] MDCG 2020-7 Post-market clinical follow-up (PMCF) Plan Template. A guide for manufacturers and notified bodies (April 2020).
[162] MDCG 2022-2 Guidance on general principles of clinical evidence for In Vitro Diagnostic medical devices (IVDs) (January 2022) 29.

The AI Act reinforces and extends these obligations. Although it does not use the terms "clinical evaluation" or "performance evaluation," the Act imposes requirements, such as accuracy, robustness, cybersecurity, transparency, human oversight, and fundamental-rights compliance, that must be verified through systematic testing. Article 9 of the AI Act obliges providers to test high-risk AI systems against predefined metrics and probabilistic thresholds, and Article 60 explicitly allows real-world testing of high-risk AI systems prior to market placement, provided that such testing complies with Union and national law, including the detailed rules of the MDR/IVDR[163].

For high-risk AI medical devices, clinical investigations and performance studies therefore serve a dual function. Firstly, they generate clinical evidence required by the MDR/IVDR, demonstrating clinical safety, performance, and benefit. Secondly, they constitute real-world testing under the AI Act, enabling verification of AI-specific requirements such as accuracy, robustness, transparency, and appropriate functioning under actual use conditions.

The alignment of these frameworks means that manufacturers conducting MDR/IVDR studies must simultaneously consider the AI Act's requirements when designing protocols, selecting datasets, defining performance metrics, and planning post-market monitoring. The AI Act's additional focus on fundamental-rights impacts, requires integrating ethical and socio-technical considerations into methodological choices typically governed by clinical research principles[164].

In sum, the MDR/IVDR and the AI Act impose complementary but distinct expectations: the MDR/IVDR ensure clinical safety and performance, while the AI Act demands demonstrable compliance with AI-specific safety, reliability, transparency, and rights-protection requirements[165]. Manufacturers must therefore adopt an integrated approach to clinical investigations and performance evaluations, ensuring that studies simultaneously satisfy the evidentiary standards of medical-device law and the technical and ethical requirements of the AI Act. In the medical devices sector, as far as data is concerned, the GDPR, MDR/IVDR, and AI Act operate cumulatively rather than hierarchically. GDPR governs whether data can be processed, MDR/IVDR ensure what evidence is needed for device approval, and the AI Act dictates how datasets must be curated to prevent bias and ensure trustworthiness.

8 Conformity Assessment and Market Access

8.1 MDR/IVDR conformity assessment and the role of notified bodies

The MDR and IVDR integrate conformity assessment as the decisive step in determining whether a product can be lawfully placed on the EU market. Conformity assessment ensures that devices meet

[163] AIB 2025-1 MDCG 2025-6, 20 (n 72).
[164] I. Kusche, 'Possible Harms of Artificial Intelligence and the EU AI Act: Fundamental Rights and Risk' (2024) Journal of Risk Research 9.
[165] E. Balogun Edmund, D. Dacosta, A. Boch, C. Luetge, 'Exploring key stakeholders' perspectives on integrating the EU AI Act with the MDR for certifying AI medical devices' (2025) 5 AI and Ethics 3001.

the GSPRs and provides the legal basis for affixing the CE marking**,** which in turn enables free circulation within the Union. The process is risk-based, with the extent of oversight scaled to the potential impact of the device on patient health and safety.

8.1.1 Risk classes and conformity pathways.

The product risk classifications under the MDR and IVDR dictate the applicable conformity assessment procedure:

- Low-risk devices (MDR Class I; IVDR Class A non-sterile, non-measuring): manufacturers may self-certify compliance with GSPRs and affix the CE mark without involvement of a notified body (NB).

- Moderate- to high-risk devices (MDR Class IIa–III; IVDR Classes B–D): assessment by a notified body is mandatory, reflecting higher regulatory scrutiny.

AI-enabled medical software frequently falls into MDR Class IIa or higher[166], and diagnostic algorithms often fall under IVDR Class C[167], both requiring NB intervention.

8.1.2 Conformity assessment and harmonised standards role

Harmonised standards play a central role in the conformity assessment of medical devices and in vitro diagnostic devices under the MDR and IVDR. While compliance with these standards is voluntary, they offer a presumption of conformity with the corresponding legal requirements, making them powerful tools for manufacturers seeking to demonstrate compliance efficiently and consistently. In practice, harmonised standards serve as the technical backbone of conformity assessment. They translate the high-level regulatory obligations of the MDR/IVDR, such as risk management, clinical evaluation, software lifecycle control, usability, and cybersecurity, into detailed, widely accepted technical specifications.

For AI medical devices, harmonised standards are even more critical. They provide structured methodologies for managing the complexity of software development, handling data quality, ensuring functional safety, and verifying and validating AI-driven decision support. Harmonised standards also facilitate a common understanding between manufacturers and notified bodies, supporting predictable, transparent conformity-assessment outcomes.

Among the most important standards that support MDR/IVDR conformity assessment are[168]:

[166] Art. 51 and Annex VIII rule 11 of the MDR.
[167] art. 47 and Annex VIII of the IVDR. Rule 1.4 of the Annex VIII states that “software, which drives a device or influences the use of a device, shall fall within the same class as the device. If the software is independent of any other device, it shall be classified in its own right.”
[168] Commission Implementing Decision (EU) 2021/1182 of 16 July 2021 on the harmonised standards for medical devices drafted in support of Regulation (EU) 2017/745 of the European Parliament and of the Council [2021] OJ L 256/100. Consolidated version: http://data.europa.eu/eli/dec_impl/2021/1182/2025-10-20 accessed 27 November 2025.

- Core safety and risk-management standards

EN ISO 14971 – Application of risk management to medical devices. Essential for identifying, evaluating, and controlling risks throughout the device lifecycle.

EN ISO 13485 – Quality management systems for medical devices. Foundational QMS standard aligned with MDR/IVDR requirements.

- Software and AI-related standards

IEC 62304 – Medical device software – Software lifecycle processes. Defines lifecycle requirements for safe software development and maintenance.

IEC/TR 80002-1 – Guidance on the application of ISO 14971 to software. Supports risk management of software-specific hazards.

IEC 82304-1 – Health software – General requirements for product safety. Covers safety and security requirements of standalone software.

- Usability and human factors

IEC 62366-1 – Application of usability engineering to medical devices. Addresses design to reduce use-errors and enhance safe interaction.

- Cybersecurity and information security

ISO/IEC 27001 and ISO/IEC 27002 – Information security management systems. Provide frameworks for protecting confidentiality, integrity, and availability of medical data.

IEC 81001-5-1 – Health software and health IT systems – Security activities. Specifically tailored to cybersecurity in health software.

- Clinical evaluation and performance evaluation

ISO 14155 – Good clinical practice for medical device investigations. Essential for designing and conducting clinical investigations under the MDR.

- Interoperability and data standards

IEC 60601 series – Medical electrical equipment (for devices integrating hardware)

8.1.3 The Role of notified bodies.

Notified bodies are independent, designated organisations authorised by national competent authorities and the European Commission to carry out conformity assessments. Their functions include:

- Reviewing technical documentation. NBs verify that manufacturers provide adequate evidence of compliance with Annex I requirements, including clinical evaluation (MDR) or performance evaluation (IVDR).

- Auditing quality management systems (QMS). They assess compliance with EN ISO 13485 and MDR/IVDR Article 10.9 QMS obligations, ensuring that processes for design, manufacture, and post-market surveillance are robust.

- Conducting product examinations. This may include sampling, type-examination, and verification of clinical or analytical performance data.

- Surveillance**.** Even after certification, NBs conduct periodic audits and unannounced inspections to verify continued conformity.

NBs thus function as gatekeepers of market access, ensuring that devices entering the EU market meet harmonised safety and performance standards.

8.1.4 CE marking and EU market access.

Once conformity is demonstrated, manufacturers may affix the CE mark, signalling compliance with EU law. CE marking authorises free movement of the device across Member States, preventing national regulatory barriers. For high-risk devices, the CE mark embodies the NB's certification of conformity, while for low-risk products it reflects manufacturer self-declaration.

8.1.5 Unique Device Identification (UDI) system.

The MDR and IVDR introduce a UDI system designed to enhance traceability and post-market surveillance[169]. Each device is assigned a unique identifier, recorded in the European database on medical devices (EUDAMED). For AI-enabled devices, the UDI system provides a critical safeguard. It allows regulators and healthcare providers to trace device versions and updates, which is particularly important where software is modified or re-trained.

8.1.6 Interaction with AI-specific requirements.

For devices incorporating AI, conformity assessment must address both frameworks, with NBs expected to verify compliance not only with GSPRs but also with AI Act obligations relating to risk management, dataset quality, and human oversight. This dual pathway underscores the need for integration between device and AI conformity documentation.

8.2 AI Act conformity assessment pathways and harmonised standards

Conformity assessment under the AI Act follows a differentiated, risk-based structure, which becomes particularly important when AI systems also qualify as medical devices or in vitro diagnostic medical devices. For high-risk AI systems in general, the AI Act provides two main pathways:

[169] Art. 27-29 of the MDR and art. 24-27 of the IVDR.

- internal control[170] and
- third-party assessment involving a notified body[171].

The pathway chosen depends on the type of high-risk AI system and the extent to which the provider relies on harmonised standards or common specifications when demonstrating compliance[172]. For AI systems listed in Annex III, point 1, which is a category that includes AI systems integrated into safety-critical applications such as medical devices, the provider may choose between internal control and notified-body involvement only when harmonised standards or applicable common specifications have been fully applied. Where standards are absent, only partially applied, or published with restrictions, or where the provider otherwise cannot rely on the presumption of conformity, the notified-body route becomes mandatory.

When an AI system falls under the MDR or IVDR, the AI Act expressly requires that the conformity-assessment procedure be carried out as part of the medical-device conformity assessment[173]. In practice, this means that the notified body designated under MDR/IVDR must also assess compliance with the AI Act's high-risk requirements, including risk management, data governance, transparency, human oversight, robustness, cybersecurity, and accuracy. It means that for AI medical devices, conformity assessment under MDR/IVDR generally fulfils AI Act requirements, provided AI Act obligations are integrated into the technical documentation and assessed by the notified body designated under MDR/IVDR. This ensures a single, integrated conformity-assessment process, preventing duplication and promoting coherence between the two regulatory regimes. As with medical-device rulemaking more broadly, any substantial modification of a high-risk AI system triggers a new conformity assessment unless the modification falls within a pre-determined change framework already validated during the initial assessment[174].

Within this structure, harmonised standards and common specifications play a decisive role. Following the Commission's Standardisation Request M/593 in May 2023 CEN- CENELEC's JTC 21 are working to finalise drafts on horizontal standards for AI quality management system, risk management, AI conformity assessment and AI trustworthiness framework[175]. When published in the Official Journal, harmonised standards will offer a presumption of conformity with the technical requirements of the AI Act. These standards help operationalise the abstract and high-level obligations of the AI Act by providing concrete methodologies for data governance, documentation, robustness testing, bias control, risk management, and cybersecurity.

If harmonised standards are delayed, incomplete, or fail to address fundamental-rights concerns, the Commission may adopt common specifications (CS). These are legally binding technical provisions that mirror the function of CS under the MDR/IVDR. AI systems conforming to these specifications also

[170] Annex VI of the AI Act.
[171] Annex VII of the AI Act.
[172] Art. 43 of the AI Act.
[173] Art. 43.3 of the AI Act.
[174] Art. 43.4 of the AI Act.
[175] Commission Implementing Decision of 22 May 2023 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence C(2023)3215 final.

benefit from a presumption of conformity; providers deviating from them must demonstrate that alternative solutions achieve an equivalent level of compliance.

For AI-enabled medical devices, the growing ecosystem of AI-specific standards being developed by CEN/CENELEC JTC 21 is expected to complement the established MDR/IVDR standards, forming a combined set of tools to guide manufacturers and notified bodies through a coherent, technically robust conformity-assessment process.

Successfully run conformity assessment is crucial in the process placing devices in the single market. Once it is completed, providers issue an EU declaration of conformity[176] and affix the CE marking[177], signalling compliance with the AI Act. For AI-enabled medical devices, CE marking already required under MDR/IVDR will be complemented by conformity with the AI Act, thereby reinforcing trust in both the clinical and technical integrity of the system.

8.3 Integration and Streamlining of Documentation (MDCG Guidance)

One of the recurring challenges in the regulation of AI-enabled medical devices is the duplication of documentation across parallel EU frameworks. As was indicated throughout this study, providers of AI-based medical devices must simultaneously demonstrate compliance with the MDR/IVDR and the AI Act, each of which imposes extensive obligations concerning technical files, risk management, quality management systems, and post-market monitoring[178]. To avoid unnecessary regulatory burden and fragmentation, the European Commission and expert bodies such as the MDCG and the AIB have emphasised opportunities for integration and streamlining of conformity documentation[179].

As was mentioned above, providers/manufacturers of the AI medical devices are required to keep and update documentation regarding their devices. Under the MDR and IVDR, documentation files must include device description, design and manufacturing information, risk management, clinical or performance evaluation data, post-market surveillance plans, and labelling/IFU materials[180]. Notified bodies review this documentation for higher-risk classes as part of the conformity assessment process.

The AI Act, in parallel, obliges providers to compile comprehensive technical documentation as well[181]. This must cover the AI system's intended purpose, system architecture, data governance, training/validation/testing datasets, risk management strategies, transparency and oversight features, and post-market monitoring mechanisms. Providers must also maintain records of algorithmic performance and logging[182].

[176] Art. 47 of the AI Act.
[177] Art. 49 of the AI Act.
[178] J. Harer, 'Post-Market Surveillance and Vigilance on the European Market' in Christian Baumgartner, Johann Harer, Jörg Schröttner (eds) Medical Devices and In Vitro Diagnostics. Requirements in Europe (Springer, Cham 2023) 585-623.
[179] AIB 2025-1 MDCG 2025-6, (n 70).
[180] Annex II-III of the MDR Annex II–III; Annex II-III of the IVDR.
[181] Art. 11; Annex IV of the AI Act.
[182] Art. 18-19 of the AI Act.

The overlap is evident: both frameworks demand lifecycle-oriented documentation capturing safety, performance, risk, and monitoring obligations, albeit with different emphases. Article 8.2 of the AI Act already acknowledges the possibility of combining obligations where devices fall simultaneously under MDR/IVDR and the AI Act. This provision reflects the principle of regulatory complementarity, allowing manufacturers/providers to integrate AI Act documentation into their MDR/IVDR files, provided that all requirements are still demonstrably satisfied.

MDCG/ AIB guidance has reinforced this integrative approach, highlighting that:

- Risk management files (ISO 14971-based under MDR/IVDR) can be expanded to cover AI Act Art. 9 requirements for risk identification, mitigation, and control across the AI lifecycle.
- Clinical evaluation reports (MDR Annex XIV) or performance evaluation reports (IVDR Annex XIII) can incorporate AI Act dataset documentation and bias analyses (Art. 10), demonstrating both clinical validity and fairness.
- Post-market surveillance plans (MDR Art. 83–86; IVDR Art. 78–81) can be harmonised with AI Act post-market monitoring systems (Art. 61), producing a single integrated monitoring plan.
- Technical documentation modules (device description, intended purpose, instructions for use) can be adapted to include AI-specific transparency obligations (Art. 13), thereby avoiding duplication.

Benefits of such a streamlined documentation are following:

- **Efficiency**: avoiding duplicative assessments may lower compliance costs and accelerate market access.

- **Clarity**: regulators, notified bodies, and competent authorities can assess a unified documentation package rather than fragmented files.

- **Lifecycle alignment**: a single set of integrated risk management, monitoring, and documentation tools enhances consistency in compliance and facilitates corrective actions.

- **Trust**: healthcare institutions and patients gain assurance that the device has been assessed holistically, covering both clinical safety and AI-specific risks.

The MDCG, together with the AI Office, is expected to issue further joint guidance clarifying best practices for integrated documentation. Early indications suggest a modular approach, where MDR/IVDR files serve as the “backbone” to which AI Act documentation can be attached. Harmonised standards and common specifications will play a critical role in ensuring that the same technical evidence (e.g., dataset validation studies, bias analyses, cybersecurity testing) satisfies both frameworks.

8.4 Cross-border trade and free movement withing the EU internal market- prevention of fragmentation across EU Member States

One of the defining objectives of EU product regulation is to facilitate free movement of goods across the internal market while maintaining high standards of safety and trust[183]. The MDR, IVDR, and AI Act all operate under the NLF model, which balances harmonisation of essential requirements at Union level with decentralised enforcement by national competent authorities. For AI-enabled medical technologies, this structure is critical to avoid regulatory fragmentation, given the sensitivity of healthcare and the diversity of national health systems.

Under the MDR and IVDR, once a device has undergone conformity assessment and the CE marking is affixed, it may circulate freely within the Union[184]. Member States may not restrict market access to CE-marked devices unless justified by serious public health grounds, thereby ensuring mutual recognition across borders. This principle is particularly important for manufacturers of AI-based medical devices, who benefit from a single harmonised route to market rather than navigating 27 different national approval regimes.

The AI Act extends this principle to high-risk AI systems, also requiring CE marking after conformity assessment[185]. By embedding AI Act compliance into the same CE marking structure, the regulation ensures that devices incorporating AI can likewise circulate freely, without Member States imposing divergent technical standards on data quality, transparency, or human oversight.

Despite harmonisation, risks of fragmentation remain. National authorities retain responsibility for designation and monitoring of notified bodies, market surveillance, and enforcement. Without coordination, Member States could apply diverging interpretations of requirements, leading to regulatory uncertainty. For instance, differences in how countries interpret "substantial modification" of an AI system[186] could fragment the market if identical software updates trigger re-certification in some jurisdictions but not in others. To counteract this, both MDR/IVDR and the AI Act rely on central coordination mechanisms:

- The MDCG issues guidance to ensure consistent application of MDR/IVDR requirements across Member States.
- The AI Office and AIB are tasked with providing interpretative guidance, coordinating supervisory practices, and facilitating standardisation under the AI Act.
- EUDAMED (for MDR/IVDR) and the EU AI database (for AI Act) further promote transparency, ensuring a common reference point for regulators and stakeholders.

[183] P. Regine, 'European Artificial Intelligence "Trusted Throughout the World": Risk-based Regulation and the Fashioning of a Competitive Common AI Market' (2024) 18(4) Regulation & Governance 1072.
[184] Art. 4 of the MDR/IVDR.
[185] Art. 48 of the AI Act.
[186] See, art. 25.1. b) of the AI Act.

Healthcare systems in the EU are largely national competences, and Member States may adopt measures to ensure safe and ethical use of devices within their borders. However, these measures cannot obstruct trade of CE-marked devices or impose parallel certification regimes. The harmonised framework thus draws a line between device conformity (EU level) and health service organisation (national level). For AI, this prevents Member States from imposing conflicting technical requirements for dataset quality, transparency, or robustness, though they may retain discretion in clinical adoption, reimbursement, and ethical oversight.

The prevention of fragmentation also strengthens the EU's position internationally. By establishing a single, harmonised set of requirements for AI-enabled medical devices, the EU creates a "gold standard" that third-country manufacturers must meet to access its market. This reinforces the Union's regulatory sovereignty and sets a benchmark for global AI and medical device governance.

9 Post-Market Obligations, Monitoring and Surveillance

9.1 Post-market surveillance under MDR and IVDR

The MDR and the IVDR establish post-market surveillance (PMS) as a cornerstone of the EU regulatory framework. Currently the set of detailed, binding obligations is imposed on manufacturers to proactively and systematically collect, analyse, and act upon data generated once devices are in real-world use. This lifecycle approach recognises that no conformity assessment can fully anticipate how a device will perform outside controlled study settings, particularly in healthcare environments where patient populations, clinical practices, and technological ecosystems evolve continuously**.**

Manufacturers are obliged to establish, document, implement, and maintain a PMS system proportionate to the device's risk class and appropriate for its type[187]. The PMS system must actively gather information from various sources, including complaints, feedback from healthcare professionals, literature reviews, registry data, and databases. Manufacturers must use this information to update benefit–risk assessments, improve usability and performance, and identify necessary corrective or preventive actions. Each device must be supported by a PMS plan, incorporated into the technical documentation[188]. This plan must describe methods and tools for:

- Collecting and analysing post-market data.
- Identifying trends in incidents or malfunctions.
- Implementing corrective and preventive measures.
- Updating clinical evaluation (MDR) or performance evaluation (IVDR) reports.

[187] Art. 83 of the MDR and art. 78 of the IVDR.
[188] Annex III of the MDR/ IVDR.

For higher-risk devices, the PMS plan must be more comprehensive, reflecting the potential impact on patient safety. AI-enabled devices, especially adaptive software, typically require robust PMS planning to monitor for algorithmic drift, performance degradation, or emergent bias.

For medium- and high-risk devices (MDR Classes IIa–III; IVDR Classes C–D), manufacturers must prepare periodic safety update reports (PSURs)[189]. They are a core element of MDR post-market surveillance and play a vital role in ensuring that a device's safety, performance, and benefit–risk profile remain acceptable throughout its lifecycle. Their primary purpose is to summarise and evaluate all post-market data, both reactive (complaints, incident reports) and proactive (literature, registries, user feedback). This is aimed at detecting any emerging trends or concerns. If new information suggests a negative shift in the benefit–risk balance, manufacturers must reassess the device in light of the clinical evaluation and risk-management processes and determine whether it continues to meet MDR requirements[190].

PSURs also serve as a structured means of reporting corrective or preventive actions (CAPA)[191], covering measures that address safety-, performance-, or quality-related issues that do not rise to the level of serious incidents or field safety corrective actions (which are reported via EUDAMED). By consolidating surveillance data, benefit–risk reassessments, and CAPA updates, PSURs provide competent authorities and notified bodies with a clear, transparent overview of real-world device behaviour. It is particularly relevant for AI-enabled medical devices, whose performance may evolve after market entry.

PSURs must be updated annually for Class III and Class D devices, and every two years for lower categories, and made available to notified bodies and competent authorities via EUDAMED. For AI-based diagnostics, PSURs may be particularly important to document performance consistency across diverse clinical settings.

The MDR/IVDR establish a vigilance system requiring manufacturers to report serious incidents and field safety corrective actions (FSCAs)[192] when devices present unacceptable risks. FSCAs may include permanent or temporary withdrawal from the market, design modifications, updated software releases, changes in labelling or instructions for use, or additional training for healthcare professionals. For software-based and AI-enabled devices, corrective actions often take the form of patches, version updates, or modifications to algorithmic models.

As it refers to incident reporting and corrective actions obligations:

- **Serious incidents** (e.g., death, serious deterioration in health, or potential for recurrence) must be reported within strict deadlines: 15 days generally, 10 days if a serious public health threat, and 2 days if death or unanticipated serious deterioration is involved.

[189] Art. 86 of the MDR and art. 81 of the IVDR.
[190] MDCG 2022-21 Guidance on Periodic Safety Update Report (PSUR) According to Regulation (EU) 2017/745 (MDR) (December 2022) 6-7.
[191] Art. 83.4 of the MDR.
[192] Art. 87-92 of the MDR and art. 82-86 of the IVDR.

- **Field safety corrective actions** (such as recalls, device modifications, or updated software patches) must be reported to competent authorities and communicated to users via field safety notices (FSNs).Such notices are to inform healthcare professionals, distributors, and users of the risks and the actions to be taken. This communication must be clear, accessible, and tailored to the urgency of the risk. In healthcare contexts, rapid dissemination of FSNs is critical to avoid repeated patient exposure to potentially unsafe AI-driven outputs.

These obligations are critical for AI-enabled devices, where a faulty algorithm could propagate systematic diagnostic errors across multiple users before detection. Prompt vigilance reporting ensures that risks are identified and mitigated before widespread harm occurs.

Manufacturers must establish systems to implement corrective actions (addressing identified problems) and preventive actions (reducing the likelihood of recurrence). This is closely linked with quality management obligations, requiring integration of PMS findings into design and manufacturing processes.

The European Database on Medical Devices (EUDAMED) plays a central role in transparency and coordination. PMS data, vigilance reports, PSURs, and FSCAs are uploaded to EUDAMED, enabling regulators, healthcare professionals, and in some cases the public to access safety information. This centralisation prevents fragmentation across Member States and facilitates cross-border vigilance for devices marketed EU-wide.

9.2 Post-market monitoring and reporting obligations under AI Act

The AI Act establishes a dedicated regime for post-market monitoring (PMM) and risk reporting for high-risk AI systems, complementing the lifecycle controls imposed at the pre-market stage[193]. While MDR and IVDR focus on clinical safety and performance, the AI Act addresses the specific risks of algorithmic systems, such as performance drift, data bias, and cybersecurity vulnerabilities[194]. Its provisions emphasise continuous oversight, traceability through logging, and structured reporting of risks to competent authorities. Providers and deployers are both subject to post-market duties.

Providers must create and document a post-market monitoring system proportional to the nature of the AI technology and the risks it poses[195]. This system must proactively and systematically collect and analyse data from deployers and other relevant sources, enabling providers to assess whether the system continues to meet the AI Act's requirements for accuracy, robustness, data governance, human oversight, cybersecurity, and overall risk control. Where applicable, this monitoring also extends to analysing how the system interacts with other AI systems. The post-market monitoring system must be grounded in a post-market monitoring plan, which forms part of the technical documentation.

[193] Art. 72 of the AI Act.
[194] A. Steimers and M. Schneider, 'Sources of Risk of AI Systems' (2022) 19 (6) International Journal of Environmental Research and Public Health 3641.
[195] C. Novelli, F. Casolari, A. Rotolo, T. Mariarosaria and L. Floridi, 'AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act' (2024) 3(1) Digital Society.

For AI systems that also qualify as medical devices or in vitro diagnostic medical devices, the AI Act allows providers to integrate AI Act–specific monitoring obligations into existing MDR/IVDR post-market surveillance and PMCF/PMPF systems. This avoids duplication and supports a unified approach to lifecycle management. As long as the combined system provides an equivalent level of protection and meets the AI Act requirements, manufacturers may embed the AI-focused monitoring activities directly into their established PMS structures. In this way, the AI Act extends the MDR/IVDR's lifecycle safety paradigm into the AI domain. Post-market monitoring becomes a dynamic, data-driven mechanism for identifying deviations in performance, detecting emerging risks, and ensuring that high-risk AI systems, including medical devices, remain safe, effective, and compliant long after they have been placed on the market[196].

Article 26 of the AI Act also imposes duties on deployers, such as hospitals and clinics. They must use AI systems in accordance with the provider's instructions, retain logs (where available), and cooperate with providers in supplying performance and incident data. This cooperation is crucial for healthcare AI, where deployers often detect anomalies, such as systematic misclassifications, that providers cannot observe directly.

A distinctive safeguard in the AI Act is the logging obligation. Keeping automatically generated logs is compulsory for providers, as well as for deployers of high-risk AI systems[197]. Article 12 requires high-risk AI systems to be designed with automatic recording of events ("logs") during operation, where technically feasible. Logs provide traceability, allowing providers, deployers, and regulators to reconstruct system behaviour and investigate the causes of adverse events. In the healthcare context, logs may capture inputs, outputs, decision pathways, or overrides, enabling audits when patient harm occurs. Logging also supports accountability by creating a verifiable record of system use.

Similarly to MDR/IVDR, the AI Act also sets rules for serious incidents reporting. Definition of 'serious incident' covers an incident or malfunctioning of an AI system that directly or indirectly leads to *inter alia* the death of a person, or serious harm to a person's health[198]. The AI Act sets out a structured risk reporting framework[199]. Providers must report to national competent authorities and market surveillance authorities any serious incidents or malfunctioning that constitute breaches of fundamental rights or safety risks. Reporting must be timely, with deadlines depending on the severity of the risk. These reports serve as an early warning mechanism, ensuring regulators can coordinate corrective measures, recalls, or prohibitions where necessary.

The AI Act emphasises that monitoring is a continuous lifecycle obligation. Providers must update technical documentation[200] and conformity assessments in the event of substantial modifications[201]. By this notion, AI Act understands "a change to an AI system after its placing on the market or putting into service which is not foreseen or planned in the initial conformity assessment carried out by the

[196] AIB 2025-1 MDCG 2025-6, 25-26 (n 72).
[197] Art. 19.1 and art. 26.6 of the AI Act.
[198] Art. 3 point 49 of the AI Act.
[199] Art. 73 of the AI Act.
[200] Art. 11 of the AI Act.
[201] Art. 43.4 of the AI Act.

provider and as a result of which the compliance of the AI system with the requirements set out in Chapter III, Section 2 is affected or results in a modification to the intended purpose for which the AI system has been assessed"[202].

Substantial modification is emerging as one of the most technically and legally sensitive junctions between the AI Act and the MDR/IVDR. Although both frameworks address modifications, the AI Act introduces its own autonomous concept of "substantial modification," which operates independently from the MDR/IVDR change-management rules, which state that any change to an approved device that may affect its safety, performance, or conditions of use must be reported to the notified body that issued the EU technical documentation assessment certificate. The notified body will determine whether the modification requires a new conformity assessment under Article 52 or can be handled through a supplement to the existing certificate. If no new assessment is needed, the notified body will review the change and, if approved, issue a supplement to the certificate[203].

Under the AI Act substantial modification is a change affecting the AI system's compliance with the high-risk requirements or its intended purpose. Crucially, art. 43.4 of the AI Act requires that any high-risk AI system. This approach recognises that even seemingly contained changes can materially alter risk profiles when algorithms are involved. The Commission will issue further guidance on how to interpret and operationalise this notion, including in the medical device context[204].

A key point of regulatory synchronisation comes from the AI Act's treatment of pre-determined changes in systems that continue to learn post-market. The Act permits providers to specify, upfront and within the technical documentation, the range of permissible adaptations expected to occur during real-world use[205]. Where such changes are pre-defined, documented, and assessed during the initial conformity assessment, they are explicitly not considered substantial modifications under the AI Act. This enables adaptive learning while safeguarding regulatory predictability.

For AI medical devices, this principle interacts directly with the MDR/IVDR. Although the MDR/IVDR do not recognise ongoing "learning" in the same way, they do require manufacturers to maintain robust change-management procedures under abovementioned Annex IX and quality system rules. The AI Act clarifies that pre-defined model updates assessed under the AIA are not treated as modifications requiring recertification under the MDR/IVDR, provided they fall within the approved design envelope. Manufacturers must ensure these pre-determined change control plans are integrated into both the AI Act technical documentation and the MDR/IVDR technical file, ensuring consistency across regulatory regimes.

A final transitional nuance concerns high-risk MDAI already on the market before the AI Act's full application. The obligations for "Annex I high-risk AI systems" only apply from 2 August 2027[206]. Thus:

[202] Art. 3 point 23 of the AI Act.
[203] Annex IX point 4.3 of the MDR, annex X point 5 of the IVDR.
[204] AIB 2025-1 MDCG 2025-6, 23 (n 72).
[205] Annex IV point 2 f) of the AI Act.
[206] AIB 2025-1 MDCG 2025-6, 23 (n 72).

If a significant change is made before 2 August 2027, the new AI Act rules on substantial modification do not yet apply.

- If a significant change is introduced on or after 2 August 2027, the AI Act applies in full, including the requirement to undergo a new conformity assessment.
- Systems placed on the market for the first time after that date must comply from the outset.

9.3 Data breach notifications and accountability under GDPR

In the domain of healthcare AI, data protection is inseparably linked with patient safety and fundamental rights. The GDPR establishes a comprehensive framework for accountability and transparency in personal data processing, with particular focus on data breach notifications. Given the sensitivity of health, genetic, and biometric data routinely processed by AI systems in clinical settings, the GDPR's enforcement architecture plays a crucial role in post-market monitoring, complementing the obligations under MDR/IVDR and the AI Act.

Under the GDPR, data controllers and data processors operating in the medical-device ecosystem, are subject to distinct yet interdependent regulatory obligations designed to safeguard individual rights and ensure responsible data governance.

Data controllers bear primary responsibility for determining the purposes and means of processing. Their obligations encompass the full spectrum of GDPR compliance: identifying a valid legal basis for processing, respecting purpose limitation, applying data-minimisation principles, and ensuring transparency toward data subjects. Controllers must also conduct DPIAs where AI-driven processing is likely to create high risks, implement appropriate technical and organisational security measures, maintain records of processing activities, and guarantee that data subject rights are fully actionable. When relying on processors, controllers must ensure that processing is governed by a binding data-processing agreement that sets out clear instructions and defines responsibilities, safeguards, and liabilities.

Data processors, by contrast, may process personal data only on documented instructions from the controller. Their obligations include implementing state-of-the-art security measures, assisting controllers in meeting GDPR requirements (such as DPIAs and responses to data-subject requests), and maintaining detailed records of processing activities carried out on behalf of controllers. Processors must also notify controllers without undue delay of any personal data breach and may not engage sub-processors without prior authorisation. Importantly, processors become directly liable under the GDPR for failing to meet their statutory duties or acting outside the controller's instructions.

In AI-enabled medical device environments, these duties acquire heightened significance. Controllers, who are often manufacturers, healthcare providers, or research institutions, must ensure that algorithmic processing complies with strict regulatory expectations, while processors, frequently cloud providers, analytics vendors, or model-training services, must implement robust technical and organisational safeguards to prevent unauthorised access, corruption, or misuse of highly sensitive medical data. Together, both actors must ensure that the lifecycle of AI medical devices operates within a compliant, transparent, and secure governance framework.

A personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data[207]. In the healthcare AI context, breaches may include unauthorised access to patient datasets used for training, disclosure of identifiable imaging data, or manipulation of clinical AI outputs due to cyberattacks. These incidents not only threaten privacy but may undermine clinical safety and trust.

Article 33 GDPR imposes a duty on controllers to notify the competent supervisory authority (usually the national data protection authority, DPA) of a personal data breach without undue delay and, where feasible, no later than 72 hours after becoming aware of it. If notification is delayed, reasons must be provided. The notification must include:

- the nature of the breach (including categories and number of affected data subjects and records),
- the likely consequences, and
- measures taken or proposed to address the breach.

For healthcare institutions deploying AI systems, this duty is particularly stringent, since breaches may have systemic effects across hospitals, networks, or national health systems. Providers/manufacturers and deployers often act as joint controllers or controller–processor pairs, requiring contractual clarity under Articles 26–28 GDPR to ensure that notification responsibilities are not neglected.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, controllers must also communicate the breach to the affected data subjects without undue delay[208]. In practice, patients must be informed if their health data has been exposed, if unauthorised parties may exploit identifiable genetic information, or if compromised AI outputs could affect clinical care decisions. Exceptions apply where risks are mitigated (e.g., through encryption) or communication would involve disproportionate effort, in which case public announcements may suffice.

Failure to comply with breach notification duties exposes organisations to severe penalties. The GDPR empowers supervisory authorities to impose administrative fines up to €10 million or 2% of global annual turnover for procedural violations (e.g., failure to notify a breach), and up to €20 million or 4% of global annual turnover for more serious violations (e.g., breaches of data subjects' rights or unlawful processing)[209]. In healthcare, such fines may apply cumulatively to providers, deployers, or processors depending on their role in the breach.

[207] Art. 4 point 12 of the GDPR.
[208] Art. 34 of the GDPR.
[209] Art. 83.4-5 of the GDPR.

9.4 Communication to patients and professionals and integrated response mechanisms

A central safeguard across frameworks is the obligation to ensure clear communication to affected stakeholders**.** Under MDR/IVDR, FSNs serve this purpose; under the AI Act, providers must inform deployers and authorities of identified risks; and under the GDPR, controllers must notify affected data subjects when personal data breaches pose high risks to their rights and freedoms. In healthcare, this convergence ensures that both professional users (clinicians, hospitals) and patients are alerted promptly when device or AI failures threaten clinical safety or data protection.

In practice, corrective actions and recalls often require coordination across legal regimes. For example, a flawed diagnostic AI may simultaneously trigger:

- an FSCA under MDR/IVDR (due to patient safety risks),
- a serious incident report under the AI Act (due to malfunction or discriminatory outputs), and
- a data breach notification under GDPR (if sensitive health data were compromised).

10 Governance, Enforcement, and Future Directions

10.1 Notified bodies under MDR/IVDR and AI Act

Notified bodies, being central regulatory authorities at the Member State level, play a fundamental role in the conformity assessment architecture of both the MDR/IVDR and the AI Act. Their functions, mandates, and scope reflect the distinct regulatory logics of medical-device law and AI governance. For AI-enabled medical devices, these two regimes increasingly intersect, making notified bodies pivotal gatekeepers of both technological safety and algorithmic trustworthiness.

Under the MDR and IVDR, notified bodies are independent, designated organisations responsible for assessing whether medical devices, other than those in the lowest risk class, meet the extensive safety, performance, and quality-management requirements of EU medical-device law. Their tasks include reviewing technical documentation, examining risk-management files, auditing quality-management systems, and evaluating clinical evidence or performance data. For software and AI-based devices, notified bodies must also assess software verification and validation, cybersecurity controls, and lifecycle management processes, including PMCF/PMPF activities. Their oversight is granular and domain-specific, reflecting the highly regulated nature of medical technologies[210].

Under the AI Act, notified bodies, also being responsible for running conformity assessment procedures, emerge in a more targeted way. Their review focuses on AI-specific requirements such as data

[210] Chapter IV of the MDR/ IVDR.

governance, transparency, documentation, human oversight, robustness, accuracy, cybersecurity, and post-market monitoring.

Crucially, for AI medical devices, the regimes converge. Article 43.3 AI Act explicitly provides that when a high-risk AI system forms part of a medical device regulated under the MDR/IVDR, the conformity assessment of AI-specific requirements is integrated into the device's existing MDR/IVDR conformity assessment. In practice, this means that the same MDR/IVDR-designated notified body, provided it meets additional competence criteria under the AI Act, assesses compliance with both frameworks. This avoids duplication, ensures consistency across overlapping requirements (e.g., risk management, software lifecycle control, clinical/performance evaluation, cybersecurity), and reinforces the principle that AI-enabled medical devices must be evaluated holistically rather than through parallel regulatory channels.

10.2 Supervisory authorities: national competent authorities, Data Protection Authorities, AI Board, MDCG

The governance of AI in healthcare within the EU is shaped by a multi-layered supervisory architecture that reflects the intersection of four major legal frameworks discussed in this study: the MDR, IVDR, GDPR, and AI Act. Each of these instruments designates specific authorities tasked with overseeing compliance, while also creating EU-level coordination bodies to ensure consistency across Member States. The result is a hybrid governance model that combines decentralised national enforcement with supranational harmonisation.

10.2.1 National competent authorities.

Under the MDR and IVDR national competent authorities (NCAs) are responsible for market surveillance, vigilance, and enforcement within their jurisdictions[211]. They monitor notified bodies, investigate non-compliance, and may take measures such as restricting or prohibiting the placing of unsafe devices on the market. For AI-enabled devices, NCAs are the first point of intervention when post-market surveillance reveals safety issues.

Particular function of national competent authorities is market surveillance. It is meant to ensure that AI-enabled medical devices remain safe, effective, and compliant throughout their lifecycle. Although the MDR/IVDR and the AI Act establish distinct surveillance regimes, they are closely aligned in purpose and increasingly interlinked for AI-driven technologies.

Under the MDR and IVDR, market surveillance authorities (MSAs) are responsible for verifying that devices placed on the EU market meet all applicable safety and performance requirements. Their powers include conducting inspections, reviewing technical documentation, performing device testing, and requiring corrective actions, where non-compliance or unacceptable risk is detected. These activities are supported by the vigilance system, manufacturer post-market surveillance obligations, PSURs, and EUDAMED reporting. For software and AI-based devices, MSAs also scrutinise cybersecurity, updates,

[211] Art. 93–100 of the MDR and art. 87-96 of the IVDR.

and change-management practices, recognising that iterative algorithmic behaviour may alter a device's risk profile after deployment.

The AI Act introduces a complementary, AI-specific market surveillance regime focusing on compliance with the high-risk AI requirements of Chapter III. MSAs may request technical documentation, demand evidence of transparency, testing, human-oversight measures, or data-governance controls, and order corrective actions where an AI system presents a risk to health, safety, or fundamental rights. Importantly, for high-risk MDAI falling under, the MDR/IVDR-designated notified bodies and MSAs retain their primary oversight role, but must integrate AI-specific controls, such as transparency, robustness, and bias mitigation, into their assessments. The AI Act expressly allows MSAs to rely on and interact with the MDR/IVDR surveillance structures to avoid duplication while ensuring AI-specific risks are addressed. NCAs also feed into EUDAMED, ensuring that vigilance data is shared at the Union level. Their work is coordinated by the MDCG to avoid regulatory divergence.

10.2.2 Medical Device Coordination Group (MDCG).

The MDCG is composed of representatives of all Member States and chaired by the European Commission. It provides guidance on the uniform application of MDR/IVDR, supports harmonisation of notified body practices, and issues interpretative documents on topics such as clinical evidence, post-market surveillance, and in-house exemptions. In the context of healthcare AI, the MDCG plays a crucial role in clarifying dual qualification issues (when an AI system is simultaneously a medical device and a high-risk AI under the AI Act) and in advising on documentation integration. Although its guidance is not legally binding, it carries significant weight in regulatory practice and in the interpretation of EU law.

10.2.3 Data Protection Authorities (GDPR).

Under the GDPR, national Data Protection Authorities (DPAs) are responsible for monitoring and enforcing compliance with data protection law[212]. They handle complaints from individuals, conduct audits, issue fines, and order corrective actions. In cross-border cases, enforcement is coordinated through the European Data Protection Board (EDPB) under the "one-stop-shop" mechanism[213]. For healthcare AI, DPAs are pivotal in overseeing sensitive health data processing, ensuring compliance with principles such as purpose limitation, minimisation, and lawfulness, and in supervising controllers' and processors' data breach notifications.

10.2.4 AI Office and European Artificial Intelligence Board.

The AI Act introduces new governance actors:

- The **AI Office**, established within the European Commission, which oversees the consistent application of the AI Act, develops guidance, and coordinates the work of notified bodies designated under the regulation.

[212] Art. 51-59 of the GDPR.
[213] Art. 60-63 of the GDPR.

- The **AIB**, composed of representatives of Member States, will mirror the function of the MDCG in the AI domain, issuing guidance, opinions, facilitating cooperation, and ensuring harmonisation.

Together, these actors are responsible for developing interpretative guidance (e.g., on substantial modifications, post-market monitoring) and for fostering convergence with existing regulatory regimes such as MDR/IVDR.

10.2.5 Complexities of multi-authority governance.

The coexistence of NCAs, DPAs, the MDCG, the AI Office, and the AIB creates a dense governance ecosystem. Overlaps are inevitable: for example, a malfunctioning diagnostic AI that leads to patient harm and exposes sensitive data may trigger investigations by NCAs (device safety), DPAs (data protection), and AI Act authorities (algorithmic risk). Effective enforcement therefore depends on institutional cooperation, information-sharing platforms, and coherent interpretative guidance[214].

The challenge ahead lies in aligning supervisory practices across these authorities, preventing regulatory fragmentation, and ensuring that compliance obligations are not duplicated or contradictory. The EU's governance architecture deliberately builds in mechanisms of coordination (MDCG, EDPB, AIB), but their effectiveness will depend on practical collaboration and the willingness of national authorities to engage in cross-regime supervision.

10.3 Enforcement mechanisms and penalties across the four regulations

The EU's legal architecture for AI in the medical devices sector rests not only on substantive obligations but also on a multi-layered enforcement system designed to secure compliance. While the MDR, IVDR, GDPR, and AI Act each operate under distinct objectives, they share a common logic: deterrence through graduated sanctions, ranging from administrative corrective measures to significant financial penalties. The diversity of enforcement mechanisms reflects the hybrid character of healthcare AI regulation, situated at the crossroads of product safety, data protection, and algorithmic governance.

10.3.1 MDR/IVDR enforcement.

Under the MDR and IVDR , enforcement is primarily carried out by NCAs, supported by market surveillance and vigilance mechanisms[215]. NCAs can:

- restrict, suspend, or withdraw devices from the market,
- prohibit or limit their availability,
- impose corrective actions, recalls, or mandatory safety updates, and

[214] C. Novelli, P. Hacker, J. Morely, J. Trondal, L. Floridi, 'A Robust Governance of the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities' (2024) European Journal of Risk Regulation 6-7.
[215] Art. 93–100 of the MDR and art. 87-96 of the IVDR.

- sanction non-compliant manufacturers, authorised representatives, or distributors.

Penalties are left to Member States , which must adopt rules that are "effective, proportionate, and dissuasive."[216] This decentralisation has led to some variation across jurisdictions, with sanctions ranging from administrative fines to criminal liability in cases of severe negligence or fraud. For AI-enabled devices, national authorities may also impose restrictions on use where software updates are deemed unsafe or substantially modified without re-certification.

10.3.2 GDPR enforcement.

As was mentioned above, the GDPR establishes one of the most far-reaching sanctioning regimes in EU law. Supervisory authorities (DPAs) may impose administrative fines under Article 83, structured into two tiers:

- Up to €10 million or 2% of global annual turnover, whichever is higher, for procedural breaches (e.g., failure to maintain records, conduct DPIAs, or notify breaches).
- Up to €20 million or 4% of global annual turnover**,** whichever is higher, for substantive violations (e.g., unlawful processing, infringement of data subjects' rights, or non-compliance with cross-border transfer rules).

Beyond fines, DPAs may order suspension of processing, erasure of unlawfully obtained data, or bans on specific AI-driven processing operations. In healthcare, where processing often involves large-scale special categories of data, GDPR enforcement serves as a powerful tool to deter negligent or exploitative data practices.

10.3.3 AI Act sanctions.

The AI Act introduces a sanctioning framework closely modelled on the GDPR, reflecting the EU's preference for high financial penalties as a compliance driver. It sets three tiers of maximum fines[217]:

- Up to €35 million or 7% of global annual turnover for breaches of prohibited practices (e.g., manipulative or exploitative AI) or non-compliance with data and transparency requirements for high-risk AI systems.
- Up to €15 million or 3% of global annual turnover for non-compliance with other AI Act obligations (e.g., QMS failures, technical documentation deficiencies, lack of post-market monitoring).
- Up to €7.5 million or 1% of global annual turnover for supplying incorrect, incomplete, or misleading information to authorities.

[216] Art. 113 MDR/ IVDR.

[217] Art. 99 of the AI Act.

Micro- and small enterprises benefit from proportionate caps, but sanctions remain substantial relative to size. Competent authorities may also order withdrawal of non-compliant AI systems from the market, suspension of deployment, or corrective modifications.

10.3.4 Comparative enforcement logic.

The four regimes reveal different enforcement emphases:

- **MDR/IVDR**: device-focused, with sanctions centred on market withdrawal, recalls, and safety corrective actions.
- **GDPR**: rights-focused, with powerful financial penalties and corrective orders targeting data processing practices.
- **AI Act**: algorithm-focused, combining GDPR-style fines with obligations tailored to continuous monitoring, robustness, and fairness.

Together, they form a composite enforcement system where non-compliance may trigger multiple sanctions simultaneously. For instance, an unsafe AI diagnostic device could prompt: a recall order under MDR, a fine under GDPR for mishandling sensitive health data, and an AI Act penalty for failure to maintain post-market monitoring. The convergence of sanctions underscores the EU's commitment to creating not only an innovation-friendly environment but also a high-accountability ecosystem for healthcare AI.

10.4 Areas of legal uncertainty and need for further guidance

Despite the ambition of the MDR, IVDR, GDPR, and AI Act to create a coherent regulatory architecture for AI in healthcare, several areas of uncertainty remain. These unresolved issues raise interpretative challenges for stakeholders and point to the need for further guidance from EU institutions, supervisory authorities, and standardisation bodies.

10.4.1 AI adaptiveness and continuous learning.

One of the most pressing uncertainties concerns the regulation of adaptive AI systems that update their performance after the market placement. The MDR and IVDR presuppose a device with relatively stable characteristics, subject to periodic post-market surveillance and updates under the manufacturer's control. By contrast, AI systems may evolve through re-training on new datasets, real-world feedback, or federated learning.

The AI Act attempts to address this by requiring new conformity assessments in cases of substantial modifications . Yet, it remains unclear where to draw the line between acceptable incremental updates (e.g., bug fixes or security patches) and modifications so fundamental that they alter the system's intended purpose or risk profile[218]. Further guidance is urgently needed to operationalise criteria for

[218] J. Laux, S. Wachter and B. Mittelstadt, 'Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and the Acceptability of Risk' (2024) 18(1) Regulation & Governance 12.

substantial modification, particularly for adaptive algorithms deployed in high-stakes healthcare contexts.

10.4.2 Secondary use of health data.

The GDPR establishes strict limits on processing health, genetic, and biometric data, permitting it only under specific legal bases. However, many AI systems depend on the availability of large, diverse datasets, including data repurposed for secondary research or algorithm training. The interplay between GDPR restrictions, national derogations for scientific research, and the European Health Data Space (EHDS) regulation[219] generates uncertainty for developers and healthcare institutions alike.

Newly adopted EHDS introduces a structured, legally harmonised framework for the secondary use of electronic health data, which has direct implications for the development, validation, and lifecycle management of AI medical device AI . While the GDPR remains the foundational regime governing personal-data processing, the EHDS establishes a dedicated mechanism for accessing and re-using health data for purposes beyond individual patient care, under strict governance and oversight. Most provisions on secondary use of health data will become applicable by 26 March 2029.

For AI medical devices sector, the EHDS will enable access to high-quality, interoperable datasets through Health Data Access Bodies (HDABs). These bodies authorise secondary-use requests for purposes such as training, testing, and validating AI models; conducting post-market performance studies; generating real-world evidence; or improving algorithmic robustness and fairness. Importantly, the EHDS prohibits the use of secondary-use data for decisions concerning individual patients, insurance assessments, or other discriminatory practices, keeping the focus squarely on research, innovation, and regulatory compliance.

The data made available under the EHDS must be processed within secure processing environments, ensuring that personal data are protected through strong technical and organisational measures, including pseudonymisation, minimisation, and strict access controls. For MDAI, this mitigates risks of data leakage, re-identification, and model-inversion attacks.

The EHDS complements the GDPR and the AI Act by providing a lawful and harmonised pathway for AI developers to access the scale and diversity of data needed to develop clinically robust algorithms, address bias, and support the regulatory requirements of MDR/IVDR and the AI Act's data-governance obligations. Yet, the framework also imposes limits: data cannot be repurposed for incompatible objectives, and all secondary-use activities must be logged, justified, and subject to oversight.

Regardless of the important step forward in the direction of controlled accessibility of health data used for secondary purposes, key questions remain: under what conditions may clinical data originally collected for treatment be repurposed for AI training? How should consent and transparency obligations

[219] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 [2025] OJ L 2025/327.

be balanced against the public interest in medical innovation? Without harmonised guidance, divergent national practices may hinder the development of robust and representative datasets, undermining both innovation and compliance[220].

10.4.3 Liability alignment.

The fragmentation of liability regimes poses another area of uncertainty. MDR and IVDR establish manufacturers' liability for defective devices under general product safety law, while the AI Act strengthens provider obligations but does not regulate the question of liability[221]. Meanwhile, the PLD reform aims to modernise liability frameworks for AI, but their final contours will be subject to interpretative debates as the ultimate model has not been determined. This creates a patchwork where manufacturers, providers, and operators, like healthcare institutions, face overlapping but not fully aligned exposures:

- Under GDPR, controllers may be liable for damages arising from data breaches or unlawful processing .
- Under MDR/IVDR, manufacturers must provide financial coverage for potential liability.
- Under the AI Act, providers may face administrative fines but not direct compensatory liability, leaving victims to rely on civil claims.

The lack of alignment raises practical concerns for patients seeking redress after harm caused by AI-enabled devices, particularly where causation is difficult to establish due to algorithmic opacity.

10.4.4 Need for interpretative guidance.

These uncertainties underscore the role of interpretative bodies such as the MDCG, the EDPB, AIB. Their guidance will be critical to:

- Clarify definitions of substantial modification for adaptive AI.
- Harmonise approaches to secondary use of health data and align them with the EHDS.
- Bridge liability gaps through interpretative opinions.

Without such guidance, stakeholders' risk inconsistent application across Member States, undermining the very goal of harmonised EU regulation.

[220] K. Söderlund, 'High-Risk AI Transparency? On Qualified Transparency Mandates for Oversight Bodies under the EU AI Act' (2025) Technology and Regulation 117.
[221] M. M. Mello and N. Guha, 'Understanding Liability Risk from Using Health Care Artificial Intelligence Tools' (2024) 390(3) New England Journal of Medicine 272.

10.5 Future convergence: toward an integrated EU framework for AI medical devices sector

The progressive densification of EU rules in the medical devices sector, with the MDR/IVDR for device safety and performance, the GDPR for data rights, and the AI Act for algorithmic trustworthiness, has produced a robust yet fragmented compliance landscape. The next phase is likely to shift from mere coexistence to institutional and procedural convergence**,** with reforms aimed at delivering a single, healthcare-tailored pathway from R&D to clinical deployment and lifecycle oversight.

A first vector of convergence is procedural integration of conformity assessment. Building on AI Act Article 8.2 (integration of documentation) and MDR/IVDR Annex II–III technical files, EU co-ordination could formalise a single dossier for AI-enabled medical technologies: one file, one quality system, mapped to MDR/IVDR GSPRs and AI Act Articles 9–15/17. This could be paired with joint assessment teams, where NBs designated under MDR/IVDR would be working alongside AI-Act-designated bodies under the guidance of the AI Office and MDCG. The benefit of such a convergence would amount to the avoidance of sequential, duplicative reviews. A unified change-management protocol would then govern "substantial modification" (AI Act) and "significant change" (MDR/IVDR guidance), creating common triggers and evidence expectations for adaptive models.

Standardisation will be the second pillar. The Commission's standardisation requests to CEN/CENELEC/ETSI can be leveraged to curate a coherent stack of harmonised standards that simultaneously satisfy AI Act and MDR/ IVDR regulations. Convergence here would let manufacturers demonstrate presumed compliance across regimes with a single test and evidence plan. As much as standardisation is an important tool supporting conformity assessment and regulatory compliance, there is a long-standing scholarly debate about the legitimacy of such a regulatory approach[222]. Standardisation, particularly in highly regulated domains such as medical devices under the MDR/IVDR and high-risk AI systems under the AI Act, it is increasingly the source of significant legal and democratic controversy[223].

A central tension stems from the outsourcing of norm-setting power. In the EU system, harmonised standards are developed not by public institutions but by private European standardisation organisations, chiefly CEN and CENELEC. For AI, this work is concentrated in the CEN-CENELEC Joint Technical Committee 21 (JTC 21). Although formally supporting EU legislation, these bodies operate through technical, consensus-based procedures that offer limited transparency and weak avenues for democratic scrutiny. The resulting standards acquire quasi-legal force: while formally voluntary, they create a presumption of conformity, effectively determining what compliance with the MDR/IVDR or the AI Act looks like in practice. This "privatisation" of regulatory detail is especially controversial in contexts where standards embed value-oriented judgments rather than purely technical specifications. Both medical devices and AI systems implicate fundamental rights, safety, equality, and human dignity.

[222] F. Palmiotto, 'The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation' (2025) 16 European Journal of Risk Regulation 781-787.
[223] T. Braun, D. E. Harasimiuk, *Legal, Regulatory and Ethical Non-binary Choices of the AI Act* (n 97) 108-113.

When standards shape how medical AI is validated, how bias is detected, or how transparency is operationalised, they influence issues traditionally governed through democratic lawmaking. Yet participation within standardisation committees remains unbalanced[224]. Empirical assessments show that industry actors dominate these bodies, while civil society, patient groups, and fundamental rights experts remain marginal. As a result, standardisation risks reflecting commercial and technical priorities more strongly than societal or ethical ones[225].

Another structural problem concerns accessibility. Harmonised standards have historically been behind paywalls, hindering public scrutiny and limiting their function as transparent legal supplements. The CJEU's landmark judgment in C-588/21 P (2024), holding that harmonised standards form part of EU law and must be freely accessible, signals a shift, but the practical implementation remains uncertain[226].

A third trajectory is data governance alignment. The EHDS envisages structured secondary use of health data for research, innovation, and regulatory purposes. Implementing acts and guidance, coordinated with the EDPB, could provide common, healthcare-specific templates for DPIAs, purpose-compatibility analyses, federated analytics, and pseudonymisation, reconciling GDPR's minimisation and purpose-limitation with AI Act dataset sufficiency and IVDR scientific/clinical performance evidence. Interoperability between EUDAMED and the EU AI database would complete the loop, enabling cross-regime traceability for software versions, model updates, incidents, and field safety actions.

The practical endpoint of these reforms is an integrated EU pathway for healthcare AI: a single documentation spine; harmonised standards mapping to all four regimes; shared assessment and post-market analytics; coordinated supervision; and aligned liability. Such convergence would lower transaction costs, accelerate safe diffusion of AI-enabled care, and strengthen trust while preserving the Union's high bar for patient safety and fundamental rights.

11 Conclusions

The analysis carried out in this Deliverable confirms that the current EU framework for AI in the medical devices sector is both substantively dense and structurally fragmented. While the cumulative application of the AI Act, MDR/IVDR and GDPR creates a high level of protection for patients and data subjects, it also generates significant duplication and overlap of regulatory requirements for manufacturers and providers. Core obligations such as risk management, post-market monitoring, documentation, transparency, human oversight and cybersecurity recure across the AI Act and MDR/IVDR and are further overlaid by GDPR duties relating to accountability, DPIAs and data security. For manufacturers/providers and healthcare deployers, this does not translate into "triple compliance" in a purely additive

[224] M. Cantero Gamito and Ch. T. Marsden, 'Artificial Intelligence Co-Regulation? The Role of Standards in the EU AI Act' (2024) 32 International Journal of Law and Information Technology 12.
[225] Corporate Europe Observatory, 'Setting the rules of their own game: how Big Tech is shaping AI standards' (7 January 2025) <https://corporateeurope.org/en/2025/01/setting-rules-their-own-game-how-big-tech-shaping-ai-standards?utm_source=chatgpt.com> accessed 14 August 2025.
[226] CJEU judgment of 5 March 2024, *Public.Resource. Org Inc., Right to Know CLG v. European Commission et al.* (Case C-588/21P, ECLI:EU:C:2024:201)

sense, but it does result in multiple, partially parallel processes (e.g. technical documentation, clinical/performance evaluation, risk assessments, FRIA/DPIA) that must be reconciled at institutional level.

This complexity is exacerbated by the immaturity of the standardisation layer under the AI Act. At the time of writing, the AI-specific harmonised standards that are intended to operationalise requirements on data governance, robustness, transparency, human oversight and bias mitigation remain under development within CEN-CENELEC JTC 21. In consequence, economic operators face a double uncertainty: on the one hand, the AI Act's high-level obligations require early compliance planning (particularly for high-risk AI medical devices from August 2027); on the other, the main technical instruments that will provide a presumption of conformity are still incomplete and normatively contested. Given the already heavy reliance of the MDR/IVDR on harmonised standards for software lifecycle, usability, clinical evidence and cybersecurity, the absence of a consolidated AI-specific standard stack risks producing inconsistent expectations among notified bodies, divergent national practices, and a "moving target" for compliance strategies.

The Deliverable also demonstrates that the overall regulatory environment is becoming increasingly opaque for stakeholders, not because individual instruments are unintelligible, but because their interaction is difficult to operationalise in a coherent way. A single actor may simultaneously be a "provider" under the AI Act, a "manufacturer" and "economic operator" under the MDR/IVDR, and a "controller" under the GDPR, a hospital may combine the roles of deployer, user, controller and, in some cases, joint controller while. Each of these roles is associated with distinct obligations, supervisory duties and potential sanctions. Without systematic internal mapping of these identities and responsibilities, there is a tangible risk that obligations will be either duplicated (leading to inefficiency and compliance fatigue) or, more problematically, fall through the cracks between regimes.

From a normative perspective, the study therefore points to a structural tension between the ambition of comprehensive protection and the realities of regulatory practice. If left unaddressed, the cumulative complexity may hinder innovation, delay market access for beneficial AI-enabled devices, and privilege large economic actors capable of absorbing high compliance costs. At the same time, any attempt to "streamline" requirements must avoid diluting the Union's protective standards for patient safety and fundamental rights. The most promising avenues, identified in the analysis, lie not in deregulation but in procedural and institutional convergence: a single integrated conformity-assessment file for AI medical devices, coordinated roles for MDR/IVDR-designated notified bodies and AI-Act-competent bodies, clearer cross-referencing between PMS/PMCF/PMPF and AI post-market monitoring, and robust, transparent governance of harmonised standards and common specifications.

Finally, the Deliverable underscores the need for sustained interpretative guidance and governance oversight. The MDCG, EDPB, AIB, AI Office and, in the medium term, the EHDS Health Data Access Bodies will play a crucial role in reducing fragmentation, clarifying grey zones (such as substantial modification, secondary use of health data for training, and the allocation of controller/processor roles), and ensuring that standardisation outputs remain aligned with fundamental rights and democratic le-

gitimacy. Future research and policy development should therefore focus on mechanisms of coordination. Only through such integrative approach the goal of fostering trustworthy AI in healthcare while maintaining a high, non-negotiable level of protection for patients and data subjects, can be achieved.

12 Bibliography

12.1 Sources of law

Commission Implementing Decision (EU) 2021/611 of 14 April 2021 amending Implementing Decision (EU) 2020/438 as regards harmonised standards on biological evaluation of medical devices, packaging for terminally sterilised medical devices, sterilisation of health care products and clinical investigation of medical devices for human subjects [2021] OJ L129/158.

Commission Implementing Decision (EU) 2021/1182 of 16 July 2021 on the harmonised standards for medical devices drafted in support of Regulation (EU) 2017/745 of the European Parliament and of the Council [2021] OJ L 256/100. Consolidated version: http://data.europa.eu/eli/dec_impl/2021/1182/2025-10-20 accessed 27 November 2025.

Commission Implementing Decision (EU) 2022/757 of 11 May 2022 amending Implementing Decision (EU) 2021/1182 as regards harmonised standards for quality management systems, sterilisation and application of risk management to medical devices [2022] OJ L 138/27.

Commission Implementing Decision of 22 May 2023 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence C(2023)3215 final.

Council Directive 93/42/EEC of 14 June 1993 concerning medical devices [1993] OJ L 169/1.

Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC [2024] OJ L 2024/2853.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) [2016] OJ L119.

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 (MDR) [2017] OJ L117/1.

Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission decision 2010/227/EU (IVDR) [2017] OJ L117/176.

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) [2024] OJ L 2024/1689.

Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 [2025] OJ L 2025/327.

12.2 Literature

Balogun Edmund E., D. Dacosta, A. Boch, C. Luetge, 'Exploring key stakeholders' perspectives on integrating the EU AI Act with the MDR for certifying AI medical devices' (2025) 5 AI and Ethics 3001.

Becker R., A. Thorogood, J. Bovenberg, C. Mitchell, A. Hall, 'Applying GDPR roles and responsibilities to scientific data sharing'(2022) 12 International Data Privacy Law 209–211, https://doi.org/10.1093/idpl/ipac011.

Braun T., D. E. Harasimiuk, *Legal, Regulatory and Ethical Non-binary Choices of the AI Act* (Routledge 2025, forthcoming).

Braun T., D.E. Harasimiuk, 'AI Deployment in Medical Devices-Ethical and Regulatory Reflections, Beyond Data Protection and Bias – EU perspective' (2023) IEEE Conference on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB), Eindhoven, Netherlands, 2023, 1-6, doi: 10.1109/CIBCB56990.2023.10264892.

Cantero Gamito M. and Ch. T. Marsden, 'Artificial Intelligence Co-Regulation? The Role of Standards in the EU AI Act' (2024) 32 International Journal of Law and Information Technology 12.

Corrales Compagnucci M., A. Dahi, and P.A Earls Davis, 'Conducting a Data Protection Impact Assessment in Health Science: A Comprehensive Guide' (November 10, 2023). Available at SSRN: https://ssrn.com/abstract=4651993 or http://dx.doi.org/10.2139/ssrn.4651993

du Boispéan S., M. Mueck, Ch. Gaie, Introduction to the European New Legislative Framework, in M. Mueck, Ch. Gaie (eds) 'European Digital Regulations' (Springer 2025) 1-19 https://doi.org/10.1007/978-3-031-80809-8

Ebers M., 'AI Robotics in Healthcare Between the EU Medical Device Regulation and the Artificial Intelligence Act. Gaps and Inconsistencies in the Protection of Patients and Care Recipients' (2024) 11 Oslo Law Review 3-4.

Ebers M., 'Truly Risk-based Regulation of Artificial Intelligence. How to Implement the EU's AI Act'. (2025) European Journal of Risk Regulation,. 16(2), 684–703. doi:10.1017/err.2024.78

Gille M., M. Tropmann-Frick and T. Schomacker, 'Balancing Public Interest, Fundamental Rights, and Innovation: The EU's Governance Model for Non;''-High-Risk AI Systems', Internet Policy Review (2024) 13(3).

Harer J., 'Post-Market Surveillance and Vigilance on the European Market' in Christian Baumgartner, Johann Harer, Jörg Schröttner (eds) Medical Devices and In Vitro Diagnostics. Requirements in Europe (Springer, Cham 2023) 585-623.

Hintze M., 'Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR' (June 7, 2018) Journal of Internet Law, Available at SSRN: http://dx.doi.org/10.2139/ssrn.3192721 accessed 23.10.2025.

Hoofnagle C. J., B. van der Sloot, & F.Z. Borgesius, 'The European Union general data protection regulation: what it is and what it means' (2019) 28(1) Information & Communications Technology Law 96–97. https://doi.org/10.1080/13600834.2019.1573501

Hornkohl L., 'The Extraterritorial Application of Statutes and Regulations in EU Law' (February 16, 2022) MPILux Research Paper 2022(1), available at SSRN: https://ssrn.com/abstract=4036688 or http://dx.doi.org/10.2139/ssrn.4036688

Kalodanis K. et al., 'Evaluating the Impact of the EU AI Act on Medical Device Regulation' in John Mantas et al. (eds), Envisioning the Future of Health Informatics and Digital Health (IOS Press 2025) 41.

Kilian R., L. Jäck, D. Ebel, 'European AI Standards-Technical Standardisation and Implementation Challenges under the EU AI Act' (2025) European Journal of Risk Regulation, 1-25.

Kusche I., 'Possible Harms of Artificial Intelligence and the EU AI Act: Fundamental Rights and Risk' (2024) Journal of Risk Research 9.

Laux J., S. Wachter and B. Mittelstadt, 'Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and the Acceptability of Risk' (2024) 18(1) Regulation & Governance 12.

Malgieri G. and F. Pasquale, 'Licensing High-Risk Artificial Intelligence: Toward Ex Ante Justification for a Disruptive Technology' (2024) 52 Computer Law & Security Review 105899.

Mantelero A., 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template' (2024) 54 Computer Law & Security Review 106020.

Mello M. M. and N. Guha, 'Understanding Liability Risk from Using Health Care Artificial Intelligence Tools' (2024) 390(3) New England Journal of Medicine 272.

Menella C.et al., 'Ethical and regulatory challenges of AI technologies in healthcare: A narrative review' (2024) 10 Heliyon e26297 doi: 10.1016/j.heliyon.2024.e26297

Meszaros J., M. C. Compagnucci, and T. Minssen, 'The Interaction of the Medical Device Regulation and the GDPR: Do European Rules on Privacy and Scientific Research Impair the Safety and Performance of AI Medical Devices?', in I.G. Cohen et al. (eds.) *The Future of Medical Device Regulation: Innovation and Protection* (2022 Cambridge University Press) 80-82.

Minghetti P. et al, 'Patient-managed digital medical devices: Do we need further regulation?' (2024) 47 Informatics in Medicine Unlocked https://doi.org/10.1016/j.imu.2024.101506

Minssen T., M. Mimler, 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 621-623.

Mühlhoff R., H. Ruschemeier, 'Updating purpose limitation for AI: a normative approach from law and philosophy' (2025) 33 International Journal of Law and Information Technologies 6-7.

Nannini L., 'When Less Regulation Means More Complexity: The EU AI Liability Directive Withdrawal and Its Impact on European Technological Competitiveness' (2025) 8 Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society 1848-61, doi:10.1609/aies.v8i2.36679.

Newdick C., 'The Development Risk Defence of the Consumer Protection Act 1987' (1988) 47 The Cambridge Law Journal 455–476. doi:10.1017/S0008197300120458.

Novelli C., F. Casolari, A. Rotolo, T. Mariarosaria and L. Floridi, 'AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act' (2024) 3(1) Digital Society.

Novelli C., P. Hacker, J. Morely, J. Trondal, L. Floridi, 'A Robust Governance of the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities' (2024) European Journal of Risk Regulation 6-7.

Ojanen A., 'Technology Neutrality as a Way to Future-Proof Regulation: The Case of the Artificial Intelligence Act'(2025) European Journal of Risk Regulation 1–2. doi:10.1017/err.2025.10024.

Onitiu D., S. Wachter, B. Mittelstadt, 'How AI challenges the medical device regulation: patient safety, benefits, and intended uses' (2024) Journal of Law and the Biosciences, lsae007, https://doi.org/10.1093/jlb/lsae007

Palmiotto F., 'The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation' (2025) 16 European Journal of Risk Regulation 781-787.

Parziale A., 'AI-powered Medical Devices and the Development Risk Defense Under the Revised Product Liability Directive' in: F. Casarosa, F. Gennari, A. Rossi, (eds) *Enabling and Safeguarding Personalized Medicine,* Data Science, Machine Intelligence, and Law (vol. 7 2025 Springer, Cham) 285. https://doi.org/10.1007/978-3-031-99709-9_14

Regine P., 'European Artificial Intelligence "Trusted Throughout the World": Risk-based Regulation and the Fashioning of a Competitive Common AI Market' (2024) 18(4) Regulation & Governance 1072.

Ruschemeier H., 'The Omnibus Package of the EU Commission Or How to Kill Data Protection Fast' (17 November 2025) <https://verfassungsblog.de/the-omnibus-package-of-the-eu-commission/> accessed 18 November 2025.

Ryngaert C., and M. Taylor, 'The GDPR as Global Data Protection Regulation?'(2020) 114 AJIL Unbound 5–9. doi:10.1017/aju.2019.80

Schütte B., ' Product Liability in the Future framework of AI (Technology) Regulation' in: M Bergström & V Mitsilegas (eds), *EU law in the digital age*, Swedish Studies in European Law (vol. 19 2025 Hart publishing) 92 https://doi.org/10.5040/9781509981212.ch-00692

Söderlund K., 'High-Risk AI Transparency? On Qualified Transparency Mandates for Oversight Bodies under the EU AI Act' (2025) Technology and Regulation 117.

Steimers A. and M. Schneider, 'Sources of Risk of AI Systems' (2022) 19 (6) International Journal of Environmental Research and Public Health 3641.

Taylor E., 'Explanation and the Right to Explanation' (2024) 10 Journal of the American Philosophical Association 467–482. doi:10.1017/apa.2023.7.

Tinabo R., F. Mtenzi and B. O'Shea, 'Anonymisation vs. Pseudonymisation: Which one is most useful for both privacy protection and usefulness of e-healthcare data' (2009) International Conference for Internet Technology and Secured Transactions, (ICITST), London, UK 1-6, doi: 10.1109/ICITST.2009.5402501.

Tomašev N. et al., 'Use of Deep Learning to Develop Continuous-Risk Models for Adverse Event Prediction from Electronic Health Records' (2021) 16(6) Nature Protocols 2785.

Vainionpää F., K. Väyrynen, A. Lanamaki, A. Bhandari, 'A Review of Challenges and Critiques of the European Artificial Intelligence Act (AIA)' (2023) *Rising like a Phoenix: Emerging from the Pandemic and Reshaping Human Endeavors with Digital Technologies ICIS 2023,* 5 <https://aisel.aisnet.org/icis2023/aiinbus/aiinbus/14> access 13.11.2025.

van Bekkum M., 'Using sensitive data to de-bias AI systems: Article 10(5) of the EU AI act' (2025) 56 Computer Law & Security Review 1-2.

van Bekkum M., F. Z. Borgesius, 'Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?'(2023) 48 Computer Law & Security Review 5-8

van Kolfschooten H., J. van Oirschot, 'The EU Artificial Intelligence Act (2024): Implications for healthcare' (2024) 149 Helath policy 105152.

van Kolfschooten H.B., 'A health-conformant reading of the GDPR's right not to be subject to automated decision-making' (2024) 32 Medical Law Review 373–391, https://doi.org/10.1093/medlaw/fwae029

Voigt P., A. von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, (Springer 2017) 87-92.

12.3 Other documents

AIB 2025-1 MDCG 2025-6, Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA), June 2025.

Art. 29 DATA PROTECTION WORKING PARTY, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216.

European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on Artificial Intelligence (Digital Omnibus on AI), COM(2025) 836 final.

Corporate Europe Observatory, 'Setting the rules of their own game: how Big Tech is shaping AI standards' (7 January 2025) <https://corporateeurope.org/en/2025/01/setting-rules-their-own-game-how-big-tech-shaping-ai-standards?utm_source=chatgpt.com> accessed 14 August 2025.

MDCG 2019-11 Rev.1, Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 –IVDR (October 2019, June 2025 rev.1). <https://health.ec.europa.eu/latest-updates/update-mdcg-2019-11-rev1-qualification-and-classification-software-regulation-eu-2017745-and-2025-06-17_en?prefLang=pl> accessed 1.10.2025.

MDCG 2020-7 Post-market clinical follow-up (PMCF) Plan Template. A guide for manufacturers and notified bodies (April 2020).

MDCG 2021-24, Guidance on classification of medical devices (October 2021)

MDCG 2022-2 Guidance on general principles of clinical evidence for In Vitro Diagnostic medical devices (IVDs) (January 2022) 29.

MDCG 2022-21 Guidance on Periodic Safety Update Report (PSUR) According to Regulation (EU) 2017/745 (MDR) (December 2022) 6-7.

MDCG 2024-3, Guidance on content of the Clinical Investigation Plan for clinical investigations of medical devices (March 2024) 6.

Recognition of EN ISO 14971 as a harmonized standard in support of the European Medical Device Regulations, <https://committee.iso.org/sites/tc210/home/news/content-left-area/news-and-updates/recognition-of-en-iso-14971-as-a.html> accessed 15 November 2025.

'The concept of 'AI system' under the new AI Act: Arguing for a Three-Factor Approach' in: *Commission Guidelines on the Application of the Definition of an AI System and the Prohibited AI Practices Established in the AI Act. Response of the European Law Institute* (2024 Vienna) 12-14. <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_on_the_definition_of_an_AI_System.pdf> access 13.11.2025.

WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Participants, Adopted by the 18th WMA General Assembly, Helsinki, Finland, June 1964, https://www.wma.net/policies-post/wma-declaration-of-helsinki/ access 20 November 2025.

12.4 Caselaw

CJEU judgment of 19 October 2016, *Breyer* (C-582/14, EU:C:2016:779);
CJEU judgment of 4 September 2025, *EDPS v SRB* (C-413/23 P, ECLI:EU:C:2025:645).
CJEU judgment of 7 December 2017, *Syndicat National de l'Industrie Des Technologies Medicales (Snitem)* (Case C-329/16, ECLI:EU:C:2017:947).
CJEU judgment of 5 March 2024, *Public. Resource. Org Inc., Right to Know CLG v. European Commission et al.* (Case C-588/21P, ECLI:EU:C:2024:201)