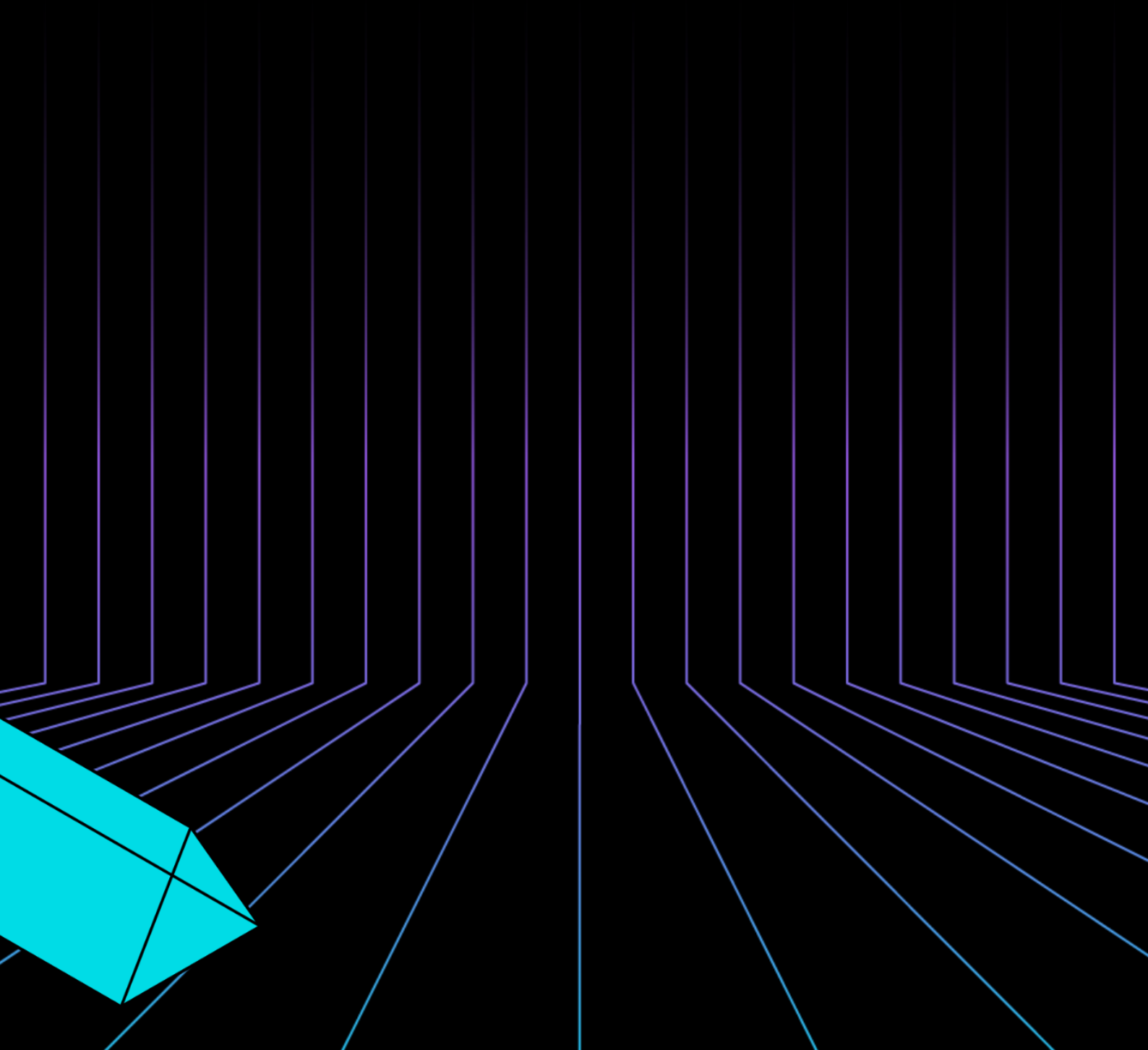
TÜV AI.LAB

Whitepaper | July 2025

AI Act and MDR – A Match Made in Heaven or Double the Trouble?



What's it All About?

Artificial Intelligence (AI) is revolutionising medicine. Already today, AI systems are used in medical practice and support healthcare professionals in diagnosis, treatment, and patient care. Innovative AI-based medical devices promise greater diagnostic precision, increased efficiency and personalised treatment approaches.

At the same time, AI-based medical devices also pose new risks such as a lack of accuracy, a lack of robustness or lead to legally prohibited discrimination. In order to address these risks and continue offering AI-based medical devices on the European market, medical device manufacturers will have to comply with a new regulation: the EU AI Act. The TÜV AI.Lab, a joint venture of five TÜV companies, is translating the regulatory requirements for AI into practice to make Europe a hotspot for safe and trustworthy AI.

Starting the 2nd of August 2027, AI-based medical devices in Europe will be subject to the dual regulatory framework: Regulation (EU) 2017/745 on medical devices (Medical Device Regulation, MDR) and Regulation (EU) 2024/1689 (Artificial Intelligence Act, AIA). The MDR, which sets out the binding requirements for medical devices for the entire European market, remains the central regulatory framework for the safety and performance of medical devices.

The AI Act, which entered into force on 1 August 2024 and is gradually taking effect, supplements this existing framework with specific requirements for the trustworthy development, use and monitoring of AI systems. It categorises AI applications according to their risk potential and defines specific due diligence obligations for high-risk AI systems - a classification that affects many medical devices with AI functionality. In combination, both legal frameworks have an impact on the trustworthiness of AI-based medical devices, the protection of patient safety and necessary clinical performance.

The parallel application of the AI Act and MDR raises significant challenges in terms of regulatory consistency and practical implementation. How are the MDR and AI Act related? What overlaps exist? What additional obligations arise for manufacturers of AI-based medical devices? These questions are at the center of the analysis below.

First, the interfaces between the central regulatory requirements of the MDR and the AI Act are critically examined, in particular their respective risk-based approaches. Next, additional obligations for manufacturers of AI-based medical devices are then identified, and key challenges as well as supportive initiatives for implementation in practice are discussed. Finally, it is demonstrated that the requirements relating to data governance, transparency and human oversight, in particular, add new dimensions to existing provisions, while requirements concerning accuracy, robustness and cybersecurity of AI systems are entirely novel.

It's a Match! What Do MDR and AI Act Have in Common?

Comparing MDR and AI Act substantial overlaps become apparent quickly. First, both the MDR and the AI Act are product regulations that harmonise the development, market placement, and operation of products across Europe. Furthermore, both legal instruments are also based on the regulatory model of the New Legislative Framework (NLF). As such, the legal text only sets out the general requirements for the respective products and providers while the technical implementation of these requirements is defined in annexes, harmonised standards, and other relevant specifications.

In addition, both legal acts require a number of key information that documents compliance with requirements relating to both the product and the manufacturing processes in question. These include, for example:

- The establishment and maintenance of an effective Quality Management System (QMS). According to Article 10(9) MDR, manufacturers must implement a QMS that covers all phases of the product life cycle. The AI Act sets out similar obligations by requiring providers of AI systems to introduce a comprehensive QMS that reflects the particular characteristics of AI systems (ref. Article 17 AIA).

- In line with the general obligations for manufacturers of medical devices under Article 10(2) MDR, manufacturers are required to establish, document, implement, and maintain a risk management system. This system serves to identify and control the risks associated with the device and is further specified in Annex I (3) MDR. The AI Act mirrors these obligations: Article 9 AIA requires the establishment, implementation, documentation, and maintenance of a risk management system designed to identify and mitigate the relevant risks of the respective AI system, particularly in relation to health, safety, and fundamental rights.

- The preparation of a Technical Documentation (TD) to demonstrate compliance with legal requirements also forms part of the manufacturers' obligations under both the MDR and the AI Act. The TD outlines the general characteristics of a system, including its intended purpose, provider, version, and hardware/software interactions. It also describes the results of the development and design processes, including the methodologies applied and other implemented safety measures.

› Post-market surveillance (PMS) constitutes another key component of both regulatory frameworks. Article 83 MDR requires manufacturers to operate a PMS system for the ongoing monitoring and evaluation of their products. The AI Act likewise mandates post-market monitoring to ensure safety and compliance under Article 72 AIA, as well as the reporting of serious incidents under Article 73 AIA.

Risk Classification of AI-Based Medical Devices under the AI Act and MDR

Both regulations adopt a risk-based regulatory approach, whereby the scope and intensity of the applicable requirements depend on the potential risks posed by the product. The higher the potential risk to users, the more stringent and comprehensive the regulatory obligations become.

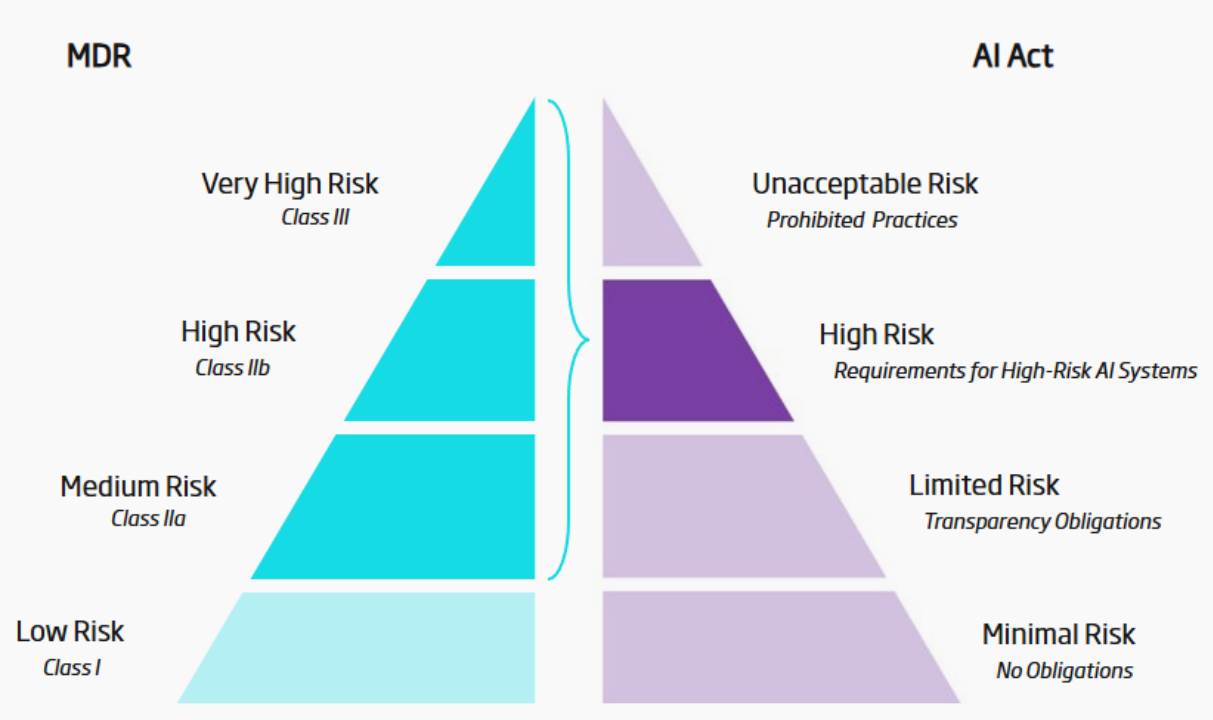


Figure 1: Schematic, simplified representation of the risk classes of the MDR (left) and AI Act (right); with the mandatory third-party review highlighted.

The MDR sets out essential safety and performance requirements for all medical devices, from Class I to Class III. Only for Class I medical devices are manufacturers permitted –under certain limitations – to place products on the European market without independent third-party assessment. From Class IIa onwards, an

independent conformity assessment by a Notified Body is required, which, in most cases, includes evaluation of both the Quality Management System and the technical documentation, particularly for AI-based medical devices. Devices classified as Class III, representing the highest level of risk, are subject to the strictest regulatory requirements, both during development and after being placed on the market. The AI Act goes even further by categorically prohibiting certain practices deemed to pose unacceptable risks for the health, safety and fundamental rights of European citizens.[1] The AI Act imposes its most comprehensive requirements on systems classified as high-risk AI. These are examined in further detail below. AI applications posing only limited risk are subject to specific transparency obligations. In contrast, minimal-risk applications are subject to no binding regulatory requirements, apart from the general obligation for providers and users to ensure that personnel involved in operating the AI systems receive appropriate training (Article 4 AIA).

Following Article 6 of the AI Act, medical devices are classified as high-risk AI systems in two instances. First, if the AI system is a standalone software product that must undergo independent third-party assessment for market authorisation according to the MDR. In line with Rule 11 on the classification of medical software, the majority of such AI-enabled medical devices may be classified as Class IIa or higher, thereby requiring a third-party conformity assessment. Second, AI-based medical devices are classified as high-risk systems under the AI Act if the AI system constitutes a safety-relevant component of a medical device that is itself subject to a third-party conformity assessment under the MDR[2]. Both scenarios operate under the assumption that products requiring independent third-party evaluation are themselves high-risk.

Furthermore, with regard to the conformity assessment itself, there is also substantial overlap between the regulatory requirements applicable to medical devices and those applicable to AI systems. These include:

- Planning and conducting a risk analysis as well as a risk assessment throughout the entire life cycle and based on the functionality, performance, and intended use of the AI-based medical device (ref. Article 9 AIA).
- Appropriate data governance during development to ensure clinical performance across different user groups (ref. Article 10 AIA).
- Validation and verification activities that demonstrate the required performance and reliability of the

[1] Furthermore, the AI Act distinguishes between AI models and AI systems. Within the meaning of the AI Act, AI systems have a specific or a general purpose. AI models are divided into those with a general purpose (with or without systemic risk) and implicitly into those without a general purpose. AI models are subject to specific requirements that are not the subject of this analysis. For an initial assessment of how the risk of AI applications can be assessed, we recommend our AI Act Risk Navigator: https://www.tuev-risk-navigator.ai

[2] The AI Act defines a safety component in Art. 3 para. 14 AIA as 'a component of a product or AI system that fulfils a safety function for that product or AI system or whose failure or malfunction endangers the health and safety of persons or property'. Whether AI systems can also function as safety components in pure software products or whether such software products as a whole are then considered "AI systems" under the AI Act is a question that requires further analysis.

AI-based medical device (ref. Article 11 AIA).

- Robust cybersecurity measures to protect AI medical devices against potential cyber threats and attacks (ref. Article 11 AIA).
- The continuous collection and evaluation of post-market surveillance data to assess the real-world performance of the AI-based medical device and to detect emerging risks as early as possible (ref. Article 72 AIA).

What's New? Additional Requirements Introduced by the AI Act

Beyond the shared regulatory foundations, the AI Act introduces a number of additional obligations that must be considered during development and deployment. For manufacturers of medical devices, this means they must not only demonstrate the patient safety and clinical performance of their devices but also comply with the specific requirements applicable to AI systems.

In particular, the AI Act sets out the following obligations for high-risk AI systems:

Requirement	Description	Impact for Medical Device Manufacturers
Art. 10 AIA Data and Data Governance	Article 10 requires that high-risk AI systems are developed using high-quality training, validation, and testing datasets, subject to appropriate data governance procedures. Bias must be mitigated, and additional safeguards must be implemented, particularly when processing special categories of personal data.	**Medium impact** Medical devices are inherently data-driven products. Consequently, strict requirements already apply under the MDR with respect to the clinical data used necessary to demonstrate clinical benefit. The AI Act, however, introduces AI-specific data governance obligations, for which neither harmonised standards nor best practices exist yet.

Art. 12 AIA Record-keeping	Article 12 establishes that high-risk AI systems must automatically log events throughout their life cycle to ensure traceability. This logging supports risk identification, post-market surveillance, and general system monitoring (ref. also Article 72 AIA).	**Medium impact** Medical device manufacturers are already obliged under MDR to record and track data on the performance of their devices as part of their post-market monitoring activitites. This is intended to help identify risks in order to ensure a continuously positive risk-benefit assessment.
Art. 13 AIA Transparency and Provision of Information to Deployers	Article 13 mandates that high-risk AI systems must be designed to ensure a sufficient degree of transparency, enabling users to interpret system outputs correctly. This aims to facilitate responsible use and human monitoring of the system.	**Minor impact** Medical device manufacturers are already obliged under MDR to provide relevant accompanying information with their product. This should help to facilitate the functionality and appropriate use for users.
Art. 14 AIA Human Oversight	Article 14 stipulates that high-risk AI systems must be designed in a way that allows for effective human oversight throughout their use. This oversight is intended to detect and mitigate risks, even when the system is used as intended.	**Medium impact** Depending on the medical device, the product is already embedded in a development process in which at least one person supervises the results of the product and can make changes. However, it is not yet clearly defined to what extent human supervision is required and how this must be implemented as a minimum for AI systems in order to sufficiently fulfil the requirements of the AI Act.

Art. 15 AIA Accuracy, Robustness and Cybersecurity	Article 15 requires high-risk AI systems to be designed and developed to ensure high levels of accuracy, robustness, and cybersecurity across their life cycle. Systems must be resistant to errors, faults, and malicious interference.	**High impact** These requirements are new for medical device manufacturers. Although they already have to perform a number of validation and verification activities to prove the accuracy of their products, testing AI systems for robustness and cybersecurity is fundamentally new.

Double the Trouble? Challenges and Unanswered Questions

The exact impact of the AI Act on the development and commercialisation of AI-based medical devices will only become apparent in the coming years. Nevertheless, certain challenges are already emerging. These include, for example:

(1) The integration of the AI Act into sector-specific regulatory frameworks. Due to the cross-sectoral nature of the AI Act, difficulties of interpretation are to be expected when integrating its horizontal requirements into sector-specific contexts. One example is the harmonisation of relevant documentation, such as the Quality Management System (QMS), Risk Management System (RMS), or Technical Documentation (TD). For example, the question arises as to how ISO 42001 and ISO 13485, as standards for AI and medical device management systems respectively, may overlap and how integrable they are.

Another example is the interpretation of the concept of a 'safety component', which plays a central role in classifying high-risk systems under the AI Act. The MDR does not explicitly define the term safety component but refers instead to device components or failures that could lead to a malfunction. It needs to be clarified how safety-relevant components in AI-based medical devices should be treated. Future steps, such as the development of harmonised standards and, in particular, the publication of guidance by the European Commission or the EU AI Office, should provide clarity.

(2) The ambiguity of innovation promotion measures. The conformity assessment procedures for medical device manufacturers are already complex. To ensure that the AI Act does not become an

additional burden–particularly for small and medium-sized enterprises the European Commission has included various innovation-enabling mechanisms directly within the Act.

One such measure is the establishment of AI regulatory sandboxes. According to Article 57(9a) of the AI Act, these sandboxes are intended to "enhance legal certainty regarding compliance with the regulatory requirements of the AI Regulation" (Article 57(9a) AIA). However, key aspects remain unclear including which stakeholders will be involved, what specific objectives the sandboxes are intended to pursue, and to what extent participation may be beneficial for different actors. In order to facilitate effective and productive collaboration across the medical sector–from manufacturers and notified bodies to competent authorities and the scientific community–concrete sandbox configurations must be developed, tested, and evaluated in practice. Timely clarification of these issues is essential to unlock the full potential of testing AI-based medical devices within a regulatory sandbox framework.

(3) The ambiguities in implementation. A regulation is only as effective as its practical implementation. For a coherent interplay between the AI Act and the Medical Device Regulation (MDR), the implementation requirements – both for manufacturers and notified bodies – must be defined as clearly and unambiguously as possible. Extending the remit of existing conformity assessment bodies currently certifying medical devices under the MDR appears to be the most pragmatic solution to minimise additional administrative burdens. Moreover, the AI Act permits small and medium-sized enterprises to adopt a simplified version of their Quality Management System, as well as the corresponding Technical Documentation (Article 11(1) AIA). However, it remains unclear how such simplified documentation will be evaluated by notified bodies, and at what point it will be considered sufficient to demonstrate the safety, performance, and trustworthiness of an AI-based medical device.

(4) The evaluation of adaptive systems. A core strength of Artificial Intelligence lies in its ability to continuously learn and adapt its outputs in response to dynamic environmental inputs. However, both the MDR and the AI Act impose strict limitations on such adaptive functionalities. Depending on the scope and nature of the modifications made to an AI-based medical device, approval by a Notified Body – or even a full reassessment of the technical documentation – may be required.

In principle, the AI Act provides the option to define anticipated modifications in advance as part of the conformity assessment procedure (ref. Recital 128 AIA). Changes that are pre-identified and pre-approved by the notified body are no longer deemed 'substantial' and may therefore be implemented without triggering a new conformity assessment.

An early practical implementation of this concept can be found in the guidance issued by the U.S. Food and Drug Administration (FDA) entitled "Marketing Submission Recommendations for a Predetermined Change

Control Plan for Artificial Intelligence-Enabled Device Software Functions"3. However, since the MDR currently does not provide a legal framework for predefining changes in a manner that would reduce their regulatory significance, it remains to be seen how such an approach could be aligned with MDR-compliant conformity pathways.

Let's Go – Innovate! A New Path Forward

The growing integration of Artificial Intelligence into medical devices holds considerable potential for enhancing diagnostics, therapy, and patient care. While the MDR and the AI Act exhibit substantial areas of overlap, the AI Act introduces a series of additional obligations specifically tailored to AI systems. In particular, the provisions concerning data governance, transparency, and human oversight introduce new regulatory dimensions. Furthermore, the requirements relating to the accuracy, robustness, and cybersecurity of AI systems represent entirely novel additions to the regulatory landscape.

To fully realise the benefits of AI in the medical context, a harmonised implementation of both regulations is essential. This requires the development of clear guidelines and standards that articulate the respective obligations and reduce interpretative ambiguities. Close cooperation between manufacturers, regulatory authorities, and notified bodies will be indispensable to ensure a smooth regulatory transition and to effectively lower barriers to innovation.

Two resources are particularly valuable in supporting this process: First, the Artificial Intelligence in Medical Devices questionnaire, published in November 2024 by Team-NB.[4] Building on preliminary work by the Interest Group of Notified Bodies (IG-NB), the questionnaire outlines process requirements relevant to the safety of AI-based medical devices. While the questions do not impose any binding legal obligations, they serve as indicators of evolving best practices.

Second, the TEF-Health project, coordinated by Charité. TEF-Health aims to reduce the time and resources required to bring AI-based medical devices to market. To achieve this, the consortium is developing a service platform specifically designed to support start-ups in navigating the regulatory landscape for AI medical devices in Europe. Although TEF-Health is scheduled to run until the end of 2027, a number of support services are already accessible to manufacturers.[5]

[3] FDA (2024): Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence-Enabled Device Software Functions, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial-intelligence
[4] Team-NB (2024): ARTIFICIAL INTELLIGENCE IN MEDICAL DEVICES, jointly published by IG-NB & Team NB, https://www.team-nb.org/medical-devices-ai-questionnaire-jointly-published-by-ig-nb-team-nb/
[5] TEF-Health Service Catalogue, https://tef-health.kg.ebrains.eu/?category=Service

In conclusion, the joint application of the MDR and the AI Act presents a unique opportunity to build trust in AI-based medical devices while simultaneously improving patient safety. Through proactive compliance efforts and ongoing multi-stakeholder dialogue, the associated challenges can be addressed and a foundation laid for innovative solutions in healthcare.

Companies that prepare early for both regulatory frameworks will not only be on secure legal ground, but will also be able to position themselves as trustworthy brands. This is especially critical in a high-risk sector such as medical devices. Alongside technological innovation, resilient regulatory and organisational structures are essential. Long-term success will ultimately depend on the capacity to build trust and demonstrate accountability. One principle remains unchanged: those who lose the trust of their customers have already lost.

TÜV
AI.LAB

TÜV AI.Lab GmbH
Max-Urich-Str. 3
13355 Berlin
Deutschland
www.tuev-lab.ai
www.tuev-risk-navigator.ai

info@tuev-lab.ai

The TÜV AI.Lab was founded in 2023 as an independent joint venture by the TÜV organisations TÜV SÜD, TÜV Rheinland, TÜV NORD, TÜV Hessen, and TÜV Thüringen. The TÜV AI.Lab aims to translate regulatory requirements for Artificial Intelligence into practical solutions and to position Europe as a leading centre for safe and trustworthy AI. To achieve this, the TÜV AI.Lab develops measurable conformity criteria and appropriate testing methods for AI systems. In addition, it actively contributes to the development of standards and norms in the field of Artificial Intelligence.