Validation of AI-Based Medical Devices

Introduction

The validation of medical devices is a crucial stage in the development and commercialization of any healthcare technology. Ensuring that a device is safe, effective, and compliant with regulatory requirements is not only a legal obligation, but also a fundamental condition for protecting both patients and healthcare professionals. In Europe, this process is governed by the Medical Device Regulation (MDR) and the In Vitro Diagnostic Medical Devices Regulation (IVDR), which establish the criteria and procedures for assessing the quality, safety, and performance of devices, including software-based ones.

In recent years, however, the technological landscape has shifted rapidly with the arrival of artificial intelligence (AI). AI is transforming entire sectors, and its integration into medical devices opens up extraordinary opportunities for diagnosis, therapy, and patient management. At the same time, it introduces new complexities for validation: algorithm-based systems that learn and adapt require more sophisticated controls to ensure transparency, traceability, and continuous risk management.

To address these challenges, the European Union has introduced the Artificial Intelligence Act (AIA), a horizontal regulation that defines harmonized rules for the use of AI in all fields. Although not designed exclusively for medical devices, the AIA fully applies when these devices incorporate artificial intelligence systems. In particular, the AIA classifies such devices as high-risk systems, imposing stringent requirements regarding safety, data governance, and human oversight.

An Integrated Regulatory Framework

To help manufacturers and authorities navigate the two regulatory systems, two bodies established by the aforementioned regulations—the Medical Device Coordination Group (MDCG) and the Artificial Intelligence Board (AIB)—have published document MDCG 2025-6. This publication provides joint guidelines that explain how to integrate the requirements of the MDR, IVDR, and AIA into the validation process for AI-based medical devices.

Risk Classification

When classifying the risk of a medical device that uses AI models, the definitions in the MDR/IVDR remain the starting point: they determine whether the integrated AI system should be considered “high risk” under the AIA, but the AIA itself does not alter the device’s class. In practice, a software application with automated diagnostic functions that falls into class IIa, IIb, or III under the MDR and requires assessment by a notified body will automatically be treated as a high-risk AI system.

Design and Development Requirements

This dual regulatory application requires manufacturers to meet a series of additional AI-specific obligations, integrating the documentation and processes mandated by the AIA into those already established for MDR/IVDR:

Management System

The MDR/IVDR requires every manufacturer to implement a quality management system and a risk management process to ensure the device's safety and performance throughout its entire life cycle.

The AIA strengthens this approach by mandating continuous, iterative risk management that includes systematic collection of post-market data, regular reviews of the AI model's performance, and thorough documentation of every change. The manufacturer must also ensure that the system enables adequate human oversight and that any model updates do not compromise safety or compliance.

Data Governance

Under the MDR/IVDR, clinical data used to evaluate a device must be robust, reliable, and representative of the target population.

The AIA introduces far more detailed requirements: training, validation, and testing datasets must be as error-free as possible, statistically representative, and supported by procedures to detect and mitigate bias. It also requires strict data governance practices, including traceability of data origins and full compliance with the GDPR.

Technical Documentation

The MDR/IVDR requires the preparation of comprehensive technical documentation describing the design, software architecture, development processes, and verification results.
The AIA expands this obligation by requiring the documentation to also include detailed information on how the AI functions, the algorithms used, performance metrics, and risk-mitigation measures, ensuring transparency and accountability.

Transparency and Human Oversight

The MDR/IVDR already requires manufacturers to provide clear instructions for use and complete information on the device's performance and limitations.

The AIA raises the level of transparency by mandating that the AI system be designed so that its decisions are interpretable and healthcare professionals can recognize when they are interacting with an algorithm. Mechanisms must also be in place to allow effective human intervention at every critical stage.

Accuracy, Robustness, and Cybersecurity

The MDR/IVDR requires devices to be safe and reliable, with adequate cybersecurity measures to prevent clinical or security risks.

The AIA aligns with these regulations and incorporates the Cyber Resilience Act, extending security measures across the entire device life cycle—from design to operational use—to prevent unauthorized access, manipulation, or "*data/model poisoning*."

Clinical Evaluation and Performance Testing

For clinical evaluation, the MDR/IVDR requires manufacturers to provide solid clinical evidence that the device is safe, performs as intended, and delivers a clinical or diagnostic benefit. This involves well-designed clinical or performance studies, rigorous data collection and analysis, and software verification and validation activities to confirm that the product meets its stated requirements.

When a device incorporates artificial intelligence, the AIA raises the bar even higher. In addition to the clinical evidence required by the MDR/IVDR, the manufacturer must:

- Validate the AI development and training processes, ensuring that the entire cycle—from design to data collection and preparation, through model training—guarantees accuracy and reliability.
- Define performance metrics and probabilistic thresholds, with testing conducted throughout development to verify that the system meets the AIA's accuracy, robustness, and safety requirements.
- Address fundamental rights, documenting that the use of AI does not create discrimination or negative impacts on individuals—an aspect not explicitly covered by the MDR/IVDR alone
- Monitor continuous learning when the algorithm is designed to update after market release, including plans to manage and validate these evolutions.

Thus, while the MDR/IVDR focuses on demonstrating clinical safety and effectiveness, the AIA adds a broader dimension: ensuring that AI remains trustworthy and aligned with ethical principles and fundamental rights throughout the device's entire life cycle.

Conformity Assessment

Every medical device must undergo a conformity assessment procedure appropriate to its risk class. In particular, devices classified as MDR class IIa or higher, or IVDR class B or higher, require the involvement of a notified body, which reviews the manufacturer's quality management system, technical documentation, and clinical evidence before granting the CE mark.

When a device incorporates an artificial intelligence system, the AIA requires that the same conformity assessment procedure also address the specific requirements for high-risk AI systems. In practice:

- The checks performed by the notified body must include compliance with Articles 8–15 of the AIA, covering aspects such as risk management, data quality, transparency, robustness, and cybersecurity.
- The technical documentation must demonstrate conformity not only with MDR/IVDR requirements but also with those of the AIA (Chapter 11, Annex IV), avoiding duplication while ensuring that both regulatory frameworks are satisfied.

In essence, for an AI-based medical device, conformity assessment is not a parallel pathway but a single integrated process, in which the MDR/IVDR review also incorporates and verifies all the additional requirements set out by the AIA.

Management of Significant Changes

The MDR/IVDR stipulates that any significant modification to a certified device—such as changes in design, software, or declared performance—must be evaluated to determine whether a new conformity procedure is required. The manufacturer must document these changes and update the risk assessment so that the notified body can decide whether the device, in its new configuration, continues to meet safety and performance requirements.

When the device incorporates artificial intelligence, the AIA introduces a specific concept of "substantial modification," broadening the focus to include less obvious but potentially critical changes for an AI system. In particular:

- Any update to the model or dataset that could influence the behavior or performance of the AI system may constitute a substantial modification and require a new conformity assessment, regardless of whether the device remains with the same deployer.
- During the initial certification phase, the manufacturer may submit a pre-determined change control plan describing expected updates and control methods; if approved, updates that adhere to this plan will not be considered substantial modifications.

Thus, while the MDR and IVDR focus on changes affecting the device's clinical or functional characteristics, the AIA extends the concept of "substantial modification" to include algorithmic updates and data changes—key factors for the safety and reliability of an evolving AI system.

Post-Market Monitoring

In the medical device sector, manufacturers must implement a robust post-market surveillance system. This means systematically collecting and analyzing data from real-world use of the device, evaluating reports of incidents or malfunctions, updating the risk assessment, and taking any necessary corrective or preventive actions.

When a device incorporates artificial intelligence, the AIA introduces additional and more targeted requirements. Beyond the activities already required by the MDR/IVDR, the manufacturer must:

- Continuously monitor the AI system's performance throughout its entire life cycle, actively documenting any deviation or anomaly from the safety, accuracy, and robustness parameters established during design.
- Prepare a dedicated post-market monitoring plan for AI, including the collection and analysis of logs and other data useful for tracking algorithm behavior and detecting bias or unexpected interactions with other AI systems.

- Promptly update the system and inform notified bodies, users, and competent authorities whenever risks emerge or corrective action is needed, while maintaining complete documentation of all actions taken.

To support this, the European Commission plans to provide a standardized post-market surveillance plan template, ensuring harmonized data collection methods and an equivalent level of protection across the Union

Conclusion

The adoption of artificial intelligence in healthcare brings extraordinary opportunities but also unprecedented regulatory challenges. The validation pathway outlined in document MDCG 2025-6 shows how the Medical Device Regulation and the Artificial Intelligence Act can work in synergy: the former ensures clinical safety and performance, while the latter addresses AI-specific risks, from data management to transparency. Only by integrating these requirements at every stage—design, development, testing, commercialization, and monitoring—can manufacturers deliver AI-based medical devices that are truly reliable and worthy of the trust of both patients and healthcare professionals.

Sources

- ***Regulation (EU) 2017/745 (MDR) – Medical Device Regulation. Official text on EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0745***
- ***Regulation (EU) 2017/746 (IVDR) – In Vitro Diagnostic Medical Devices Regulation. Official text on EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0746***
- ***Regulation (EU) 2024/1689 (Artificial Intelligence Act – AIA) – Artificial Intelligence Regulation. Official text: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689***
- ***Medical Device Coordination Group (MDCG) 2025-6 – Interplay between the MDR/IVDR and the Artificial Intelligence Act***