TÜV AI.LAB

Whitepaper | June 2025

Better Safe Than Sorry? ISO 13485 and the EU AI Act

Executive Summary

Artificial Intelligence has already found its way into medical technology – but its full market potential is yet to be realised. One key reason: the regulatory requirements for high risk systems are extensive. In addition to the obligations of the Medical Device Regulation (MDR), the European AI Act (EU 2024/1689) also mandates a comprehensive Quality Management System (QMS) for high-risk AI systems.

This white paper explores the extent to which ISO 13485 – as an established standard for medical devices – fulfils the new requirements of the AI Act (AIA). The findings reveal that many provisions of Art. 17 AIA, such as those relating to development, quality assurance and communication with authorities, are already comprehensively addressed. However, AI-specific aspects such as data governance or AI-related risk management are not inherently covered.

The good news: there is no need to build an entirely new second Quality Management System from scratch. Instead, existing ISO 13485 systems can be purposefully expanded. This allows companies to meet regulatory requirements without duplicating structures.

The white paper provides practical guidance for manufacturers operating at the intersection of the MDR and the AI Act, illustrating how an evolutionarily enhanced QMS can serve as a bridge between the two regulatory frameworks.

QMS – A New Era?

AI systems have long been an integral part of innovative medical devices, and their potential is vast: they support the recognition of patterns in image data, help streamline diagnostic processes and assist in therapeutic decision-making. For healthcare professionals, who are often stretched to their limits, this means support, relief, and opportunities for efficiency gains and qualitative consistency. However, the number of AI-based medical devices actually available on the European market remains limited – a broad market rollout is still in its early stages.

One of the key requirements for authorisation in accordance with the Medical Device Regulation (EU) 2017/745 (MDR) is generally a robust Quality Management System (QMS). For medical devices, the structure is typically based on ISO 13485[1]. As a harmonised standard, it helps manufacturers to establish processes and activities to meet the regulatory requirements of the MDR. However, the upcoming regulation on artificial intelligence EU 2024/1689, the European AI Act, will add additional requirements for QM systems for providers of high-risk AI systems.

But what specific requirements does the AI Act (AIA) place on QM systems? Is a QM system set up according to ISO 13485 sufficient to meet the AI Act's demands – or must an entirely separate QM system be established? These are the questions this paper seeks to address. First, it examines the specific QMS requirements set out by the AI Act. A comparative analysis then evaluates how ISO 13485 aligns with these requirements.

The findings show that ISO 13485 largely meets the general QM system requirements outlined in the AI Act. However, due to its technology-agnostic nature, there are AI-specific gaps that must be specifically addressed. This can be done through a targeted

[1] Reference is hereby made to the German edition of EN ISO 13485:2016, Medical devices – Quality management systems – Requirements for regulatory purpose.

expansion of the QM system in accordance with ISO 13485, so that the creation of an additional QM system is not necessary. Regulatory conformity is therefore possible with limited effort.

Requirements for Quality Management Systems under the AI Act

The AI Act sets out specific requirements for QM systems of AI providers in Art. 17. Their implementation should be proportionate to the size of the respective organisation (Art. 17(2) AIA) and may be integrated into existing QM systems (Art. 17(3) AIA). In doing so, the legislator acknowledges the demands from industry stakeholders for a balanced approach regarding the associated administrative and organisational burden.

The QMS of a provider of high-risk AI systems must systematically map central requirements in accordance with Art. 17 (1) AIA. The requirements mentioned in this paragraph include, for example, a concept for compliance with regulatory requirements, including conformity assessment and change management. In addition, suitable procedures for design, development, quality control and quality assurance must be demonstrated and the development phases must be safeguarded by validated inspection and test procedures. Technical specifications and applicable standards must also be named and checked for their suitability to fulfil the essential requirements.

Of particular importance are the following elements: a Risk Management System in accordance with Art. 9 AIA, a post-market monitoring system as required by Art. 72 AIA and a procedure for reporting serious incidents pursuant to Art. 73 AIA. A detailed overview of the requirements under Art. 17 AIA can be found in the Annex.

Article 17 AI Act in Relation to ISO 13485

A comparison of the requirements set out in Art. 17 AIA with those of ISO 13485 reveals that, while certain aspects are fully addressed, others remain insufficiently covered. This outcome is primarily attributable to the technology-agnostic nature of ISO 13485, which does not explicitly encompass AI-specific considerations. The detailed analysis is as follows:

Table 1: Comparison of Quality Management System Requirements between Article 17(1) AIA and ISO 13485

AI Act Reference[2]	ISO 13485	Coverage Ratio[3]	Brief Justification
Art. 17 (1) (a)	**4.1.4** Regulatory Requirements **5.6** Management Review **7.3.9** Control of Design and Development Changes	**Partial**	ISO 13485 requires compliance with regulatory requirements and mandates their implementation within the Quality Management System. However, it does not provide for a strategically documented overarching responsibility for compliance with the AI Act, nor does it include AI-specific policies or formal change management processes.
Art. 17 (1) (b)	**7.1** Planning of Product Realisation	**Full**	ISO 13485 requires planned product realisation including the necessary verification and validation activities in this phase and thus covers Art. 17 (1) (b).
Art. 17 (1) (c)	**7.3.1 - 7.3.7** Design and Development	**Full**	The standard specifies procedures for development control, qualified personnel and documented quality control and assurance. The requirements for systematic development and production processes are thus covered.

[2] A detailed overview of the requirements under Art. 17 AIA can be found in the Annex.
[3] Coverage Ratio Legend: Full – ISO 13485 fully aligns with the requirements of the AI Act. Partial – A process exists, but it does not fully meet the requirements. Gap – ISO 13485 does not address the topic, or covers it only marginally.

Art. 17 (1) (d)	**7.3.1 - 7.3.7** Design and Development **7.5** Production and Service Provision **8.1-8.2** Measurement, Analysis and Improvement	**Full**	Validation and verification activities ensuring the required safety and performance based on the functional specifications of the medical device are fully addressed by the standard.
Art. 17 (1) (e)	**4.1.4** Regulatory Requirements **7.3.3** Design and Development Inputs	**Partial**	ISO 13485 requires the consideration of regulatory and functional requirements. However, it does not include documentation of data and data governance, record-keeping obligations, human oversight, or requirements for accuracy, robustness, and cybersecurity as set out in Chapter III, Section 2 of the AI Act.
Art. 17 (1) (f)	-	**Gap**	ISO 13485 addresses data usage primarily in the context of design inputs. However, it does not include a structured data management system with defined processes for data collection, cleaning, labelling, or ingestion into AI models.
Art. 17 (1) (g)	**7.1** Planning incl. reference to ISO 14971	**Partial**	ISO 13485 explicitly requires the integration of risk management processes and references ISO 14971[4]. While commonly applied to software-based products, it does not account for AI-specific risks. According to the MDR, manufacturers can refer to a risk-benefit ratio, while the AI Act largely only considers the risk.

[4] Where ISO 13485 refers to the risk management process, this process must be aligned with the risk concept as defined by the MDR, i.e. to reduce risk "as far as possible and appropriate" (cf. ISO 13485, Annex ZB).

Art. 17 (1) (h)	**8.2.1** Feedback **8.5** Improvement	**Partial**	ISO 13485 prescribes a post-market surveillance framework aimed at ensuring ongoing product conformity. However, the specific elements set out in Annex VI(3) AIA, which are essential to post-market monitoring, are not explicitly covered and would need to be added.
Art. 17 (1) (i)	**8.2.3** Reporting to Regulatory Authorities	**Full**	Incidents affecting product safety or compliance must be reported to the competent authorities under ISO 13485. These obligations align with the requirements set out in the AI Act.
Art. 17 (1) (j)	**7.2.3** Communication	**Full**	The standard defines clear communication processes with competent authorities, notified bodies and customers. The systematic exchange must be documented and regulated in a comprehensible manner.
Art. 17 (1) (k)	**4.2.5** Control of Records	**Full**	Documentation requirements and control of records are comprehensively regulated under ISO 13485. Auditability and traceability are normative obligations, satisfying the requirements of the AI Act.
Art. 17 (1) (l)	**6.1 - 6.4** Resource Management **7.4** Purchasing	**Full**	ISO 13485 covers personnel, infrastructure, supporting services, working environment, and suppliers. These elements are fully aligned with the AI Act's expectations.
Art. 17 (1) (m)	**5.5** Responsibility, Authority and Communication	**Partial**	Roles and responsibilities must be defined by the organisation. However, they are not specifically delineated for AI-related applications.

Conclusion: Between Synergy and Additional Effort – What Lies Ahead?

The AI Act stipulates the establishment of a Quality Management System as a central means of demonstrating compliance with regulatory requirements. In this context, ISO 13485, the key QMS standard for medical devices, demonstrates a high degree of structural compatibility with the requirements set forth in the AI Act.

However, the analysis also reveals gaps in ISO 13485 with regard to AI-specific characteristics. These gaps can be attributed to the technology-agnostic yet sector-specific nature of the Medical Device Regulation (MDR), which applies to medical devices classified from Class I to III, encompassing both software and physical products. This nature is reflected in ISO 13485, which is aligned with the same product categories. In contrast, the AI Act adopts a technology-specific but cross-sectoral approach, thereby complementing the MDR[5]. The aforementioned gaps between ISO 13485 and the AI Act are therefore both expected and specific.

For manufacturers already operating a QMS in conformity with ISO 13485, the AI Act does not necessitate a fundamental departure from their existing systems. Rather, targeted enhancements will be required. These enhancements primarily concern those areas where AI systems fundamentally differ from traditional, rule-based software products– whether deployed as stand-alone applications or as safety components embedded in physical devices.

For example, while ISO 13485 requires a structured product development process and change control, it does not differentiate between AI-based and conventional systems. Modifications to an AI system–such as retraining using updated datasets–are subject to

[5] While AI technologies are understood here as a single term, in practice these technologies are, of course, highly diverse and entail their own specific requirements.

different dynamics and risks compared to changes in traditional software, and therefore demand additional AI-specific governance mechanisms.

Another illustrative case is data management. Although ISO 13485 includes requirements for the validation of design inputs, it lacks concrete provisions for processes such as data annotation, data cleansing, or measures to control bias and discrimination– each of which is critical to the performance and safety of AI-based systems.

A potential pathway to extending existing QM system structures is expected to emerge with the publication of harmonised standards specifically developed to facilitate implementation of the AI Act within the European regulatory framework. In particular, the draft standards JT021024 - EN AI Risk Management and JT021039 - EN Quality Management System for EU AI Act Regulatory Purposes are of relevance. However, these are still in the early stages of development and are not expected to be finalised until mid-2026, according to the official timeline.

In the meantime, the application of ISO 42001 presents a viable opportunity to close the AI-specific gaps between the AI Act and ISO 13485. ISO 42001 has been developed specifically as a management standard for AI applications (AIMS) and therefore addresses use cases that are directly relevant to AI. It contains specific provisions relating to AI roles, AI-related risks, and initial guidance on the implementation of AI-specific control mechanisms.

In summary, ISO 13485 provides a structurally compatible foundation for meeting the QMS requirements of the AI Act. In this respect, the AI Act fulfils its stated aim of avoiding regulatory duplication. For manufacturers, compliance is achievable through targeted extensions addressing AI-specific issues, without the need to establish an entirely new QM system.

Annex

Table 1: Requirements of the AI Act for QMS pursuant to Article 17(1)

Art. 17 (1)	Requirement
(a)	A strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system
(b)	Techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system
(c)	Techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system
(d)	Examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out
(e)	Technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full or do not cover all of the relevant requirements set out in Section 2, the means to be used to ensure that the high-risk AI system complies with those requirements
(f)	Systems and procedures for data management, including data acquisition, data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purpose of the placing on the market or the putting into service of high-risk AI systems
(g)	The risk management system referred to in Art. 9 AIA
(h)	The setting-up, implementation and maintenance of a post-market monitoring system, in accordance with Art. 72 AIA
(i)	Procedures related to the reporting of a serious incident in accordance with Art. 73 AIA
(j)	The handling of communication with national competent authorities, other relevant authorities, including those providing or supporting the access to data, notified bodies, other operators, customers or other interested parties
(k)	Systems and procedures for record-keeping of all relevant documentation and information
(l)	Resource management, including security-of-supply related measures
(m)	An accountability framework setting out the responsibilities of the management and other staff with regard to all the aspects listed in this paragraph

TÜV
AI.LAB

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