Gap Analysis of Standards for EU AI Act Compliance for healthcare

Artificial Intelligence – Task 2

Mid-Phase Report

Table of Contents

1. Executive Summary

1.1. Purpose and scope of the gap analysis

This gap assessment is specifically focused on standards that apply to **Medical Devices**, **In Vitro Diagnostics (IVDs)**, and which incorporating **Artificial Intelligence (AI)** technologies. The primary objective is to identify gaps in existing standards and ensure alignment with emerging regulatory requirements.

In the next phase of the Report, it is planned to include Healthcare Delivery Organizations.

The scope includes:

- **High-risk AI systems** as defined under the **EU AI Act**, where only medical devices fall within the assessment perimeter.
- **Low to moderate-risk health applications** that have a **medical purpose or which are classified as medical devices** and are utilized within healthcare settings.

This assessment aims to support standardization efforts and provide clarity on compliance standards for AI-enabled medical technologies. It will serve as a foundation for future standardization activities to address safety and performance in this rapidly evolving domain.

1.2. Out of Scope

As part of this assessment, circularity considerations are addressed under Task 1, focusing on principles that promote resource efficiency and lifecycle management for AI-enabled medical technologies

It is important to note that the European Health Data Space (EHDS) and all associated regulations, including any standards required for their implementation, are explicitly excluded from the scope of this assessment. These areas fall outside the defined objectives and will not be addressed within the current gap analysis.

1.3. Key Findings and Recommendations

After extensive discussions and the remarkable efforts of the group, we have identified several key recommendations that we believe can play a vital role in fostering innovation, safety, and collaboration across Europe. Looking ahead, we would like to share the following, where we concentrate on Medical Device Manufacturers. In the next phase we plan to add healthcare providers as well.

1. **Extension of the Group's Mandate**
   The current mandate of this group is limited to two years. However, as most relevant standards are still under development within SC42, JTC 21, and SC62, we strongly recommend extending the group's work for at least another two years to ensure continuity and effectiveness.

2. **Volume and Complexity of Standards**
   Our analysis shows that there is a large volume, to this topic relevant, standards published or under development:
   SC42 / JTC 1:
   • 41 standards published
   • 47 standards under development
   JTC 21:
   • 12 SC42 standards published as EN
   • 3 EU-specific standards published
   • 18 standards under development

   Given this large volume, it is unrealistic for medical device manufacturers to participate in all standardization activities during the development phase of these standards. Therefore, we propose focusing on reviewing finalized standards and then defining their applicability to medical devices and publishing consolidated guidance documents.

3. **Balanced Approach to Standardization**
   While we appreciate the impressive speed of new standardization activities, we recommend a balanced approach to maintain clarity and avoid overwhelming implementers. Quality must remain the highest priority. We recognize the urgency created by the AI Act, but the number of experts capable of interpreting and implementing these standards within companies is limited.

4. **Structured Roadmap**
   A well-defined roadmap with clear priorities will help focus resources, maximize impact, and foster sustainable growth for all stakeholders.

5. Harmonization of upcoming international standards:
   The "IEC PAS 63621 ED1 Artificial intelligence enabled medical devices - Data management" is a Public Available Specification, which could not be harmonized due the Art of standard.
   Ensure that also this kind of standards could be harmonized.

2. Roadmap for Compliance

2.1. Short-term actions (0–12 months)

Harmonize the upcoming standards:

- IEC PAS 63621 Artificial intelligence enabled medical devices - Data management
  Release planned for Q1 of 2026

- ISO 24971-2 Medical devices — Guidance on the application of ISO 14971 - Part 2: Machine learning in artificial intelligence

- Release underway current limit date January 5th 2026

- PT 63450 Artificial Intelligence-enabled Medical Devices – Methods for the Technical Verification and Validation
  Release planned End of 2026

Send Experts to the following projects:

- ISO 20417 Medical devices — Information to be supplied by the manufacture (upcoming)

- IEC TS 62366-3 Medical devices — Part 3: Guidance on the application of usability engineering to medical devices using artificial intelligence and machine learning technology

2.2. Medium-term actions (1–3 years)

- Enrich QMS with the necessary processes incl. Post Market Surveillance and purchasing processes

- Follow the JTC21 standards and the regulatory changes as necessary

- Write on Cen Cenelec TC62 recommendations which standard are useful for medical devices

- Start the project for Cen Cenelec 62 an TC 62 simultaneously
  - Data Model for the technical documentation of medical devices and specifications
  - IEC 62304 Medical device software — Software life cycle processes
  - AAMI CR515:2025; Cybersecurity considerations unique to machine learning–enabled medical devices

2.3. Long-term strategy (beyond 2027)

This chapter will be included in the final report.

3. Introduction

3.1. Overview of the EU AI Act in Healthcare

The EU Artificial Intelligence Act (AI Act), which entered into force in August 2024, represents the world's first comprehensive legal framework for AI. It adopts a risk-based approach, classifying healthcare AI systems—such as diagnostic tools, treatment decision support, and surgical robotics—as high-risk due to their direct impact on patient safety and fundamental rights. This classification imposes strict requirements: robust risk management, high-quality and unbiased datasets, transparency and explainability, and meaningful human oversight. Compliance also includes technical documentation and post-market monitoring. While these obligations increase complexity for developers and healthcare providers, they aim to foster trust, safety, and accountability. The Act's extraterritorial reach ensures global alignment, similar to GDPR, positioning Europe as a leader in ethical AI governance. For healthcare, this framework is both a challenge and an opportunity: it sets clear guardrails while encouraging innovation that prioritizes patient well-being.

3.2. Importance of Harmonized Technical Standards

Harmonized technical standards are essential for translating the AI Act's and MDR/IVDR principles into practical compliance. They provide a common language for safety, interoperability, and transparency across borders and sectors. In healthcare, where data fragmentation and diverse regulatory environments pose significant hurdles, standards such as EN Standards based on ISO, IEC, and emerging EU-specific Standards ensure consistent quality, risk management and safe and effective products. The effect of fast and reliable harmonization of international standards is, that it reduces duplication of effort, lowers compliance costs, and accelerates market access by enabling conformity assessments. Beyond regulatory alignment, harmonized standards build trust among clinicians and patients by guaranteeing that AI systems meet agreed benchmarks for performance and security. Without these standards, the promise of AI in healthcare—improved diagnostics, operational efficiency, and personalized care—will remain fragmented and unevenly implemented.

3.3. Methodology of the Gap Analysis

The gap analysis methodology begins with defining scope and objectives: identifying which standards and regulatory requirements apply to healthcare AI systems under the EU AI Act. For this year we concentrate on the medical device manufacturers. The process involves comparing current practices against these requirements to pinpoint areas of full compliance, partial alignment, or complete gaps. Typically, this is structured through checklists or matrices aligned with harmonized standards. Key steps include:

1. mapping existing processes and documentation,
2. assessing risk management and data governance practices,
3. evaluating transparency and human oversight measures,
4. prioritizing corrective actions based on risk and resource impact.

The outcome is a clear roadmap for achieving compliance, supporting both regulatory readiness and continuous improvement. This structured approach not only mitigates legal and operational risks but also strengthens organizational confidence in deploying compliant and trustworthy AI solutions.

3.4. Use Case Applications in Healthcare

AI is already delivering tangible benefits in European healthcare. Leading use cases include medical imaging and diagnostics, where AI enhances accuracy in radiology and pathology, enabling earlier detection of conditions such as breast cancer. Predictive analytics supports hospital resource management by forecasting admissions and optimizing bed allocation. Administrative automation—such as digital scribes and documentation tools—reduces clinician workload, freeing time for patient care. In intensive care, AI models predict sepsis onset hours before symptoms appear, improving survival rates. Pharmaceutical innovation also benefits, with AI accelerating drug discovery and personalized medicine development. While adoption remains uneven due to data silos, resource availability and regulatory complexity, these examples demonstrate AI's potential to improve outcomes, efficiency, and sustainability when integrated responsibly into clinical workflows.

3.5. Regulatory Framework

The regulatory framework for artificial intelligence (AI) and machine learning (ML) in medical devices is shaped by a combination of international standards, European Union legislation, and national regulations. Key elements include:

- **EU Medical Device Regulation (MDR) and In Vitro Diagnostic Regulation (IVDR):** These regulations establish requirements for safety, performance, and clinical evaluation of devices incorporating AI. Manufacturers must ensure compliance with essential requirements, including risk management and transparency.
- **AI Act (Proposed EU Regulation):** The forthcoming AI Act introduces a risk-based approach to AI systems, classifying medical AI as high-risk. It mandates conformity assessments, documentation of algorithms, and post-market monitoring to ensure ongoing compliance.
- **Harmonized Standards and Guidance:** Standards such as ISO 13485 (Quality Management), IEC 62304 (Software Lifecycle), and ISO 14971 (Risk Management) provide structured methodologies for integrating AI into medical devices.

This framework ensures that AI-enabled medical devices meet stringent safety, performance, and accountability criteria, fostering trust and innovation in healthcare.

3.6. Timeline and Applicability of the EU AI Act

The EU AI Act entered into force on 1 August 2024, marking a historic step in global AI governance. Its provisions apply progressively over several years to allow stakeholders time to adapt. Key milestones include: prohibitions on certain "unacceptable risk" AI systems and AI literacy requirements from February 2025, obligations for general-purpose AI (GPAI) models from August 2025, and the bulk of high-risk system requirements from August 2026. Full enforcement, including penalties, is expected by August 2027, though recent discussions suggest possible grace periods for compliance to avoid market disruption. The Act applies extraterritorially, meaning any provider or user whose AI outputs affect EU residents must comply, regardless of location. This phased approach balances regulatory certainty with innovation, giving companies time to implement robust governance while ensuring that safety and fundamental rights remain central to AI deployment.

The Digital Omnibus, published on the EU Commission website, introduces targeted adjustments to facilitate the implementation of the AI Act. These changes include extended compliance timelines for high-risk AI systems, simplified registration requirements, and streamlined conformity assessment procedures. For CEN-CENELEC, this means accelerating the development and delivery of harmonized standards through JTC 21 to align with the revised framework and ensure industry readiness under the updated regulatory conditions with extended timelines.

3.7. Classification of AI Systems (e.g., High-Risk, GPAI)

The EU AI Act adopts a risk-based classification system to tailor obligations to potential harm. AI systems fall into four categories:

Unacceptable risk: Prohibited outright (e.g., social scoring, manipulative AI).

High-risk systems: Applications with significant impact on health, safety, or fundamental rights—such as medical devices (according to MDR / IVDR) , biometric identification, and critical infrastructure—subject to strict compliance requirements including conformity assessment, risk management, and human oversight.

Limited risk: Systems requiring transparency (e.g., chatbots, deepfakes) to inform users they are interacting with AI.

Minimal risk: Most consumer AI applications, with no additional obligations. In addition, General-Purpose AI (GPAI) models—large-scale models capable of diverse tasks—are regulated separately. GPAI providers must maintain technical documentation, disclose training data summaries, and implement cybersecurity and systemic risk measures. This classification ensures proportionate regulation: stringent for high-impact systems, lighter for low-risk applications, fostering both trust and innovation.

3.8. Legal Obligations for Providers and Users

Under the AI Act, providers—those who develop or market AI systems—bear the most extensive obligations. For high-risk systems, these include:

- Implementing a risk management system and ensuring high-quality and unbiased datasets.
- Preparing technical documentation and registering systems in the EU database.
- Conducting conformity assessments before market entry and maintaining post-market monitoring.

Ensuring human oversight, robustness, and cybersecurity. For GPAI providers, obligations extend to publishing training data summaries, complying with copyright rules, and performing systemic risk evaluations.
Users (deployers) also have responsibilities: operating systems according to instructions, monitoring performance, and reporting serious incidents. Transparency duties apply when interacting with individuals or using emotion recognition or biometric categorization. These obligations aim to create a culture of accountability across the AI value chain, ensuring safe and ethical deployment while enabling innovation under clear, harmonized rules.

3.9. Existing International and European standards (ISO, IEC, IEEE)

Number	Standard	IEC SC 42	JTC 21	Applicable for Medical manufacturer
ISO/IEC TS 4213 2022	Information technology — Artificial intelligence — Assessment of machine learning classification performance	Published	-	Yes applicable for medical
ISO/IEC 5259-1: 2024	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 1: Overview, terminology, and examples	Published	Published	-
ISO/IEC 5259-2: 2024	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 2: Data quality measures	Published	Published	Partially
ISO/IEC 5259-3 2024	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 3: Data quality management requirements and guidelines	Published	Published	Not Evaluated
ISO/IEC 5259-4 2024	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 4: Data quality process framework	Published	Published	With changes
ISO/IEC 5259-5 2025	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 5: Data quality governance framework	Published	-	Not Evaluated
ISO/IEC 5338 2023	Information technology — Artificial intelligence — AI system life cycle processes	Published	-	Not applicable
ISO/IEC 5339 2024	Information technology — Artificial intelligence — Guidance for AI applications	Published	-	Not Evaluated
ISO/IEC 5392:2024	Information technology — Artificial intelligence — Reference architecture of knowledge engineering	Published	-	Not Evaluated
ISO/IEC TR 5469:2024	Artificial intelligence — Functional safety and AI systems	Published	-	Not Applicable
ISO/IEC TS 6254 2025	Information technology — Artificial intelligence — Objectives and approaches for explainability and interpretability of machine learning (ML) models and artificial intelligence (AI) systems	Published	-	Not Evaluated
ISO/IEC 8183 2023	Information technology — Artificial intelligence — Data life cycle framework	Published	Published	Not applicable
ISO/IEC TS 8200 2024	Information technology — Artificial intelligence — Controllability of automated artificial intelligence systems	Published	-	

Number	Standard	IEC SC 42	JTC 21	Applicable for Medical manufacturer
ISO/IECTS 12791 2024	Information technology — Artificial intelligence — Treatment of unwanted bias in classification and regression machine learning tasks	Published	Published	Not Evaluated
ISO/IECTR 17903 2024	Information technology — Artificial intelligence — Overview of machine learning computing devices	Published	-	
ISO/IECTR 20226 2025	Information technology — Artificial intelligence — Environmental sustainability aspects of AI systems	Published	-	Not Evaluated
ISO/IEC 20546 2019	Information technology — Big data — Overview and vocabulary	Published	-	Not Applicable
ISO/IEC TR 20547-1 2020	Information technology — Big data reference architecture — Part 1: Framework and application process	Published	-	Not Applicable
ISO/IEC TR 20547-2 2018	Information technology — Big data reference architecture — Part 2: Use cases and derived requirements	Published	-	Not Applicable
ISO/IEC 20547-3 2020	Information technology — Big data reference architecture — Part 3: Reference architecture	Published	-	Not Applicable
ISO/IEC TR 20547-5 2018	Information technology — Big data reference architecture — Part 5: Standards roadmap	Published	-	Not Applicable
ISO/IEC TR 21221 2025	Information technology — Artificial intelligence — Beneficial AI systems	Published	-	
ISO/IEC 22989 2022	Information technology — Artificial intelligence — Artificial intelligence concepts and terminology	Published	Published	IMDRF overrules
ISO/IEC 23053 2022	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)	Published	Published	
ISO/IEC 23894 2023	Information technology — Artificial intelligence — Guidance on risk management	Published	Published	Not Applicable
ISO/IEC TR 24027 2021	Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making	Published	Published	Not Evaluated
ISO/IEC TR 24028 2020	Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence	Published	-	Not Evaluated
ISO/IEC TR 24029-1 2021	Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview	Published	Published	Not Evaluated

Number	Standard	IEC SC 42	JTC 21	Applicable for Medical manufacturer
ISO/IEC 24029-2 2023	Artificial intelligence (AI) — Assessment of the robustness of neural networks — Part 2: Methodology for the use of formal methods	Published	-	Not Evaluated
ISO/IEC TR 24030 2024	Information technology — Artificial intelligence (AI) — Use cases	Published	-	Not Evaluated
ISO/IEC TR 24368 2022	Information technology — Artificial intelligence — Overview of ethical and societal concerns	Published	-	Not Evaluated
ISO/IEC TR 24372 2021	Information technology — Artificial intelligence (AI) — Overview of computational approaches for AI systems	Published	-	Not Evaluated
ISO/IEC 24668 2022	Information technology — Artificial intelligence — Process management framework for big data analytics	Published	-	Not Evaluated
ISO/IEC TS 25058 2024	Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guidance for quality evaluation of artificial intelligence (AI) systems	Published	-	Not Evaluated
ISO/IEC 25059 2023	Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality model for AI systems	Published	Published	Not Evaluated
ISO/IEC 38507 2022	Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations	Published	-	Not Applicable
ISO/IEC 42001 2023	Information technology — Artificial intelligence — Management system	Published	Under Approval	Not Applicable
ISO/IEC 42005 2025	Information technology — Artificial intelligence (AI) — AI system impact assessment	Published	-	Not Applicable
ISO/IEC 42006 2025	Information technology — Artificial intelligence — Requirements for bodies providing audit and certification of artificial intelligence management systems	Published	-	Not Applicable
ISO/IEC CD 4213	Artificial intelligence — Performance measurement for AI classification, regression, clustering and recommendation tasks	Under Development	-	Applicable
ISO/IEC CD TR 5259-6	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 6: Visualization framework for data quality	Under Development	-	Not Evaluated
ISO/IEC 12792	Information technology — Artificial intelligence — Transparency taxonomy of AI systems	Under Development	Approved	Not Evaluated

Number	Standard	IEC SC 42	JTC 21	Applicable for Medical manufacturer
ISO/IEC CD TR 18988	Artificial intelligence — Application of AI technologies in health informatics	Under Development	-	Not Evaluated
ISO/IEC AWI TS 22440-1	Artificial intelligence — Functional safety and AI systems — Part 1: Requirements	Under Development	-	Not Evaluated
ISO/IEC AWI TS 22440-2	Artificial intelligence — Functional safety and AI systems — Part 2: Guidance	Under Development	-	Not Evaluated
ISO/IEC AWI TS 22440-3	Artificial intelligence — Functional safety and AI systems — Part 3: Examples of application	Under Development	-	Not Evaluated
ISO/IEC CD TS 22443	Information technology — Artificial intelligence — Guidance on addressing societal concerns and ethical considerations	Under Development	-	
ISO/IEC AWI 22989-2	Artificial intelligence — Concepts and terminology — Part 2: Healthcare	Under Development	-	
ISO/IEC 22989:2022/DAmd 1	Information technology — Artificial intelligence — Artificial intelligence concepts and terminology — Amendment 1: Generative AI	Under Development	Under Enquiry	
ISO/IEC 23053:2022/DAmd 1	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) — Amendment 1: Generative AI	Under Development	Under Enquiry	
ISO/IEC CD TR 23281	Artificial intelligence — Overview of AI tasks and functionalities related to natural language processing	Under Development	Under Drafting	
ISO/IEC CD 23282	Artificial Intelligence — Evaluation methods for accurate natural language processing systems	Under Development	-	
ISO/IEC CD 24029-3	Artificial intelligence (AI) — Assessment of the robustness of neural networks — Part 3: Methodology for the use of statistical methods	Under Development	-	
ISO/IEC AWI TR 24030	Information technology — Artificial intelligence (AI) — Use cases	Under Development	-	
ISO/IEC DIS 24970	Artificial intelligence — AI system logging	Under Development	Under Drafting	
ISO/IEC CD 25029	Artificial intelligence — AI-enhanced nudging	Under Development	-	Not Applicable

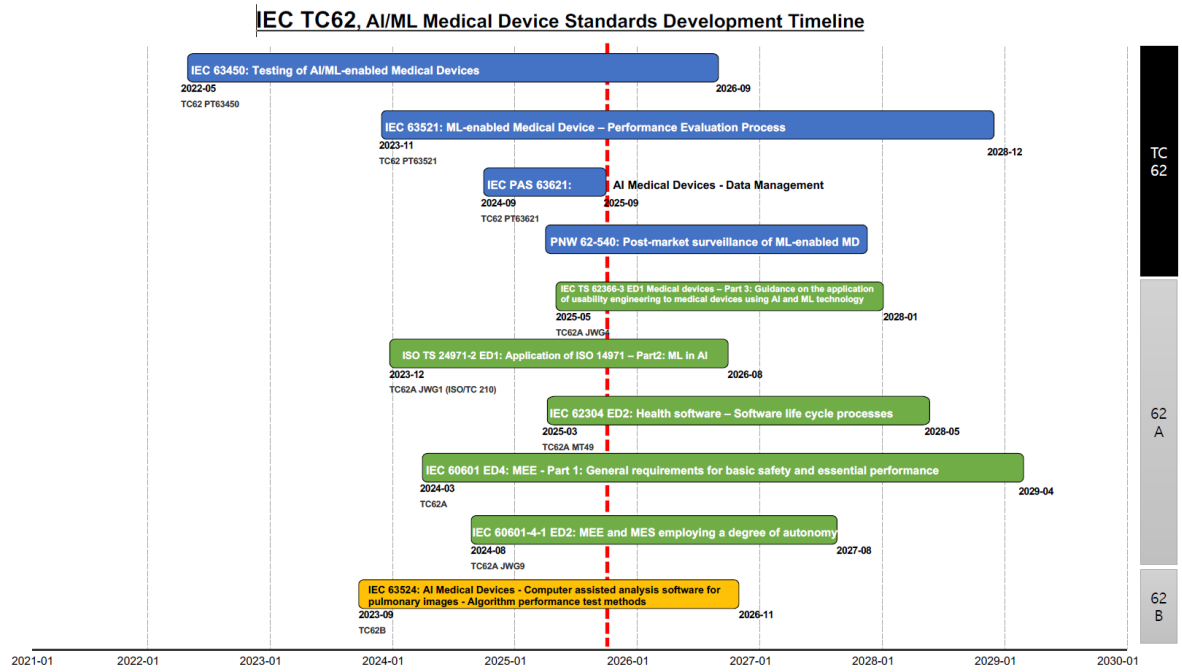
Number	Standard	IEC SC 42	JTC 21	Applicable for Medical manufacturer
ISO/IEC AWI 25058	Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Measurement and guidance for quality evaluation of AI systems	Under Development	-	Not Applicable
ISO/IEC CD 25059	Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality models for AI systems	Under Development	Under Drafting	Not Applicable
ISO/IEC AWI TS 25223	Information technology — Artificial intelligence — Guidance and requirements for uncertainty quantification in AI systems	Under Development	-	
ISO/IEC AWI TS 25258	Information technology — Artificial intelligence — Hybrid AI inference framework for AI systems	Under Development	-	
ISO/IEC AWI TR 25523	Information technology — Artificial intelligence — Overview of data profiles for analytics and ML	Under Development	-	
ISO/IEC AWI TS 25566	Terminology and concepts for domain engineering of AI systems	Under Development	-	
ISO/IEC AWI TS 25568	Information technology — Artificial Intelligence — Guidance on addressing risks in generative AI systems	Under Development	-	
ISO/IEC AWI TS 25569	Artificial Intelligence — Implementation guidance on de-identification of data used in Machine Learning (ML)	Under Development	-	
ISO/IEC AWI TS 25570	Information Technology — Artificial Intelligence — Reliability assessment of AI systems	Under Development	-	
ISO/IEC AWI TS 25571	Artificial Intelligence — Example template for documenting ethical issues of an AI system	Under Development	-	
ISO/IEC AWI 25589	Information technology — Artificial intelligence — Framework for human-machine teaming	Under Development	-	
ISO/IEC AWI 25590	Information technology — Artificial intelligence — Guidance for output data quality of generative AIapplications	Under Development	-	
ISO/IEC AWI 25623	Artificial intelligence — Machine learning (ML) model description framework	Under Development	-	
ISO/IEC AWI 25704	Artificial Intelligence — Process assessment model for AI system life cycle processes	Under Development	-	

Number	Standard	IEC SC 42	JTC 21	Applicable for Medical manufacturer
ISO/IEC AWI 25870	Artificial intelligence — Reporting framework for AI incidents	Under Development	-	
ISO/IEC AWI 25872-1	Artificial intelligence — Knowledge enhancement for pretrained machine learning models — Part 1: Framework	Under Development	-	
ISO/IEC AWI 42003	Information technology — Artificial intelligence — Guidance on the implementation of ISO/IEC 42001	Under Development	-	
ISO/IEC AWI 42007	Information technology — Artificial intelligence — High-level framework and guidance for the development of conformity assessment schemes for AI systems	Under Development	-	
ISO/IEC CD 42102	Information technology — Artificial intelligence — Framework for characterizing AI system methods and capabilities	Under Development	Under Drafting	
ISO/IEC AWI TR 42103	Information technology — Artificial intelligence — Overview of synthetic data in the context of AI systems	Under Development	-	
ISO/IEC DIS 42105	Information technology — Artificial intelligence — Guidance for human oversight of AI systems	Under Development	-	
ISO/IEC DTR 42106	Information technology — Artificial intelligence — Overview of differentiated benchmarking of AI system quality characteristics	Under Development	-	
ISO/IEC AWI TR 42109	Information technology — Artificial intelligence — Use cases of human-machine teaming	Under Development	-	
ISO/IEC AWI TS 42111	Information technology — Artificial intelligence — Guidance on lightweight AI systems	Under Development	-	
ISO/IEC CD TS 42112	Information technology — Artificial intelligence — Guidance on machine learning model training efficiency optimization	Under Development	-	
ISO/IEC TS 42119-2	Artificial intelligence — Testing of AI — Part 2: Overview of testing AI systems	Under Development	-	
ISO/IEC DTS 42119-3	Artificial intelligence — Testing of AI — Part 3: Verification and validation analysis of AI systems	Under Development	-	
ISO/IEC AWI TS 42119-7	Artificial intelligence — Testing of AI — Part 7: Red teaming	Under Development	-	

Number	Standard	IEC SC 42	JTC 21	Applicable for Medical manufacturer
ISO/IEC AWI TS 42119-8	Artificial intelligence — Testing of AI — Part 8: Quality assessment of prompt-based text-to-text systems that utilize generative AI	Under Development	-	
CEN/CLC/TR 17894:2024	(WI=JT021001) Artificial Intelligence - Artificial Intelligence Conformity Assessment	-	published	
CEN/CLC/TR 18115:2024	Data governance and quality for AI within the European context	-	published	
CEN/CLC/TR 18145:2025	(WI=JT021010) Environmentally sustainable Artificial Intelligence	-	published	
prCEN/CLC/TR XXX	(WI=JT021009) AI Risks - Check List for AI Risks Management	-	Preliminary	
prCEN/CLC/TR XXX	(WI=JT021026) Impact assessment in the context of the EU Fundamental Rights	-	Preliminary	
prCEN/TS	(WI=JT021033) Guidance for upskilling organisations on AI ethics and social concerns	-	Preliminary	
prCEN/TS	(WI=JT021034) Guidelines on tools for handling ethical issues in AI system life cycle	-	Preliminary	
prEN 18228	(WI=JT021024 AI Risk Management	-	Preliminary	
prEN 18229-1	(WI=JT021008) I trustworthiness framework – Part 1: Logging, transparency and human oversight	-	Under Drafting	
prEN 18229-2	(WI=JT021047) AI trustworthiness framework – Part 2: Accuracy and robustness	-	Under Drafting	
prEN 18274	(WI=JT021019) Competence requirements for professional AI ethicists	-	Under Drafting	
prEN ISO/IEC 23282	(WI=JT021012) Artificial Intelligence - Evaluation methods for accurate natural language processing systems	-	Under Drafting	
prEN ISO/IEC 25029	(WI=JT021046) Artificial intelligence - AI-enhanced nudging	-	Under Drafting	
prEN XXX	(WI=JT021039) Artificial intelligence - Quality management system for EU AI Act regulatory purposes	-	Under Drafting	
prEN XXX	(WI=JT021036) Artificial Intelligence - Concepts, measures and requirements for managing bias in AI systems	-	Under Drafting	
prEN XXX	(WI=JT021037) Artificial Intelligence -- Quality and governance of datasets in AI	-	Under Drafting	

Number	Standard	IEC SC 42	JTC 21	Applicable for Medical manufacturer
prEN XXX	(WI=JT021029) Artificial intelligence - Cybersecurity specifications for AI Systems	-	Under Drafting	
prEN XXX	(WI=JT021044) Artificial Intelligence - Taxonomy of AI tasks in computer vision	-	Under Drafting	
prEN XXX	(WI=JT021038) AI Conformity assessment framework	-	Under Drafting	
prEN XXX	(WI=JT021025) Artificial Intelligence – Evaluation methods for accurate computer vision systems	-	Under Drafting	
	(WI=JT021030) Contributions towards ISO/IEC 27090	-	Preliminary	
prCEN/TS	(WI=JT021035) Sustainable Artificial Intelligence – Guidelines and metrics for the environmental impact of artificial intelligence systems and services	-	Under Drafting	

3.10. Existing international standards (ISO, IEC, IEEE) for Medical Devices



Project	Status
IEC 63450 ED1 Testing of Artificial Intelligence / Machine Learning-enabled Medical Devices	CDV in preparation
IEC 63621 PAS Data Management for AI enabled medical devices	DPAS in preparation
ISO TS 24971-2 ED1 Medical devices – Guidance on the application of ISO 14971 - Part 2: Machine learning in artificial intelligence	DTS approved
IEC 63524 ED1 Artificial Intelligence enabled Medical Devices — Computer assisted analysis software for pulmonary images - Algorithm performance test methods	CDV approved
IEC 63521 ED1 Machine Learning-enabled Medical Device – Performance Evaluation Process	CD commenting phase closed, not yet decided if there will be a CD2 or a CDV
IEC TS 62366-2 ED1 Medical devices – Part 3: Guidance on the application of usability engineering to medical devices using artificial intelligence and machine learning technology	CD expected this year
AI Annex for IEC 62304 ED2 Medical device software - Software life cycle processes	Part of the CD for IEC 62304 (62A/1639/CD), CD2 expected Start of 2026
PNW 62-540 ED1(IEC/IEEE 63685): Post-market surveillance of machine learning-enabled medical devices	CD expected beginning of next year (IEEE has approved to establish JWG)
IECEE pilot “AI components for medical devices”	Approved, the project is currently in a preliminary phase

4. Key Compliance Domains

The following compliance domains represent critical pillars for ensuring that AI-enabled medical devices meet regulatory, ethical, and technical requirements. Each domain aligns with European legislation, international standards, and emerging best practices.

4.1. Risk Management and Mitigation

Risk management is a foundational requirement under MDR, IVDR, and ISO 14971. Manufacturers must identify hazards associated with AI systems, assess their probability and severity, implement risk-mitigation strategies, and perform benefit-risk analysis throughout the lifecycle. This includes:

- **Pre-market risk analysis**: Evaluating algorithmic risks such as bias, overfitting, and underfitting, dataset imbalance, and model drift or instability.
- **Post-market surveillance**: Continuous monitoring for performance degradation and emerging risks in real-world use.
- **Dynamic risk controls**: Updating models and controls based on real-world data.

Effective risk management ensures patient safety and regulatory compliance, particularly for high-risk AI systems under the EU AI Act.

4.2. Data Governance and Quality (including fairness, bias, ethics)

Data governance is essential for ensuring the integrity and fairness of AI systems. Key principles include:

- **Data quality and representativeness**: Training datasets must reflect clinical diversity to avoid bias.
- **Ethical compliance**: Adherence to GDPR and ethical guidelines for patient data protection.
- **Bias and fairness audits**: Regular assessments to detect and mitigate discriminatory outcomes.
- **Traceability**: Documenting data sources, preprocessing steps, and validation procedures.

Strong governance frameworks foster trust and align with both MDR/IVDR and AI Act requirements for transparency and accountability.

4.3. Transparency and Explainability

Transparency is critical for regulatory approval and clinical acceptance. AI systems must provide:

- **Clear documentation**: Including algorithm choice and/or design, training methodology, and performance metrics, including justifications for metrics selected.
- **Explainability tools**: Enabling clinicians to understand decision-making processes.
- **Regulatory alignment**: Meeting AI Act obligations for transparency and user information.

Explainability supports human oversight and mitigates risks associated with opaque decision-making.

4.4. Human Oversight and Control

Human oversight ensures that AI systems operate under meaningful human control. Requirements include:

- **Override and stop mechanisms**: Allowing natural persons to interpret, intervene, and override or halt the system when necessary.
- **Decision support**: AI should augment, not replace, human judgment while final responsibility remains with the human operator .
- **Training and competence**: Ensuring Users to be adequately trained to understand the system's capabilities, limitations, and risks, including how to detect malfunction or misuse.
- Awareness of automation bias: Oversight must include the ability to monitor and counter over-reliance on AI outputs.
- Monitoring and Logging: The Act mandates that AI systems must have the technical capabilities for recording events to facilitate human oversight and monitoring. This includes logs that can help identify potential risks and allow for future review of system functioning.

These measures ensure meaningful human control, reduce automation bias, and safeguard patient safety and fundamental rights.

4.5. Robustness, Accuracy, and Cybersecurity

AI systems must demonstrate resilience against errors and malicious attacks. Compliance involves:

- **Robustness testing**: Validating performance under varied clinical conditions.
- **Accuracy verification**: Continuous evaluation against ground truth data.
- **Cybersecurity measures**: Implementing IEC 81001-5-1 IEC TR 60601-4-5, IEC 62304 to protect data and system integrity and security.

Robustness and security are essential for maintaining trust and regulatory conformity.

4.6. Fundamental Rights Impact Assessment

The AI Act mandates an assessment of potential impacts on fundamental rights, to evaluate how the system may affect individuals' rights and freedoms before it is placed on the market, including privacy, non-discrimination, and patient autonomy. This involves:

- **Impact analysis**: Identifying risks to fundamental rights: Assess potential impacts on privacy, non-discrimination, equality, autonomy, health, and safety
- **Vulnerable groups**: Evaluate how certain populations may be disproportionately affected by outputs or decision pathways.
- **Mitigation strategies**: Implementing safeguards to prevent harm, including measures and arrangements for European governance and complaint mechanisms.

- **Documentation**: Providing evidence of compliance for regulatory review.

This assessment ensures ethical deployment and societal acceptance of AI technologies.

4.7. Conformity Assessment for Certification (CE Mark)

Conformity assessment is the final step in demonstrating compliance with MDR, IVDR, and AI Act requirements. Key elements include:

- **Technical documentation**: Comprehensive evidence of safety, performance, and risk management, data governance, human oversight, AI-specific requirements, including Quality Management System employed.
- **Notified body review**: Independent evaluation of conformity.
- **Harmonized standards**: Leveraging ISO 13485, IEC 62304, IEC 82304-1and other emerging AI-specific standards.

Successful conformity assessment enables CE marking, ensuring market access, safety assurance and regulatory trust.

5. Key Compliance for Healthcare Organizations

Healthcare organizations, particularly hospitals, play a critical role in ensuring that AI-enabled medical devices are deployed safely and ethically. Compliance in this context extends beyond device certification to organizational governance, risk management, and quality assurance.

5.1. Guidance for Hospitals

Hospitals must establish internal governance structures to manage AI systems effectively. Key actions include:

- **Policy development**: Define clear policies for AI adoption, covering procurement, validation, and clinical integration.
- **Training and competence**: Ensure clinicians and technical staff understand AI system capabilities, limitations, and associated risks.
- **Monitoring and reporting**: Implement processes for continuous performance monitoring and incident reporting to comply with MDR and AI Act obligations.
- **Ethical oversight**: Establish ethics committees or advisory boards to review AI use cases, ensuring alignment with patient rights and societal values.

These measures help hospitals maintain accountability and patient safety while leveraging AI innovations.

5.2. ISO 42001 QMS Use in Hospitals

ISO/IEC 42001 introduces a Quality Management System (QMS) tailored for AI. Hospitals adopting this standard benefit from:

- **Structured governance**: A framework for managing AI lifecycle activities, including risk assessment and performance evaluation.
- **Integration with existing QMS**: Harmonization with ISO 9001 and ISO 13485 for seamless compliance.
- **Continuous improvement**: Mechanisms for iterative updates based on clinical feedback and technological advancements.
- **Audit readiness**: Documentation and traceability to support regulatory audits and certification processes.

Implementing ISO 42001 enhances organizational resilience and ensures conformity with emerging AI-specific requirements.

5.3. Risk Management in Hospitals

Risk management within hospitals focuses on operational and clinical risks associated with AI deployment. Key components include:

- **Clinical risk assessment**: Evaluating potential impacts on patient safety, diagnostic accuracy, and treatment outcomes.
- **Operational risk controls**: Addressing risks related to system integration, cybersecurity, and data governance.
- **Incident response protocols**: Establishing clear procedures for handling AI-related failures or adverse events.
- **Stakeholder engagement**: Involving clinicians, IT teams, and patients in risk identification and mitigation strategies.

Effective risk management ensures that hospitals maintain compliance while safeguarding trust in AI-driven healthcare.

6. Gap Identification

6.1. Mapping existing standards to EU AI Act requirements

This chapter will be included in the final report.

6.2. Areas lacking sufficient standardisation

This chapter will be included in the final report.

6.3. Challenges in interpretation and implementation

This chapter will be included in the final report.

7. Technical Documentation Requirements

7.1. Technical Documentation Requirements

This chapter will be included in the final report.

8. Lifecycle traceability and version control

Effective lifecycle traceability and version control ensure that every element of an AI-enabled medical device, such as requirements, datasets, algorithms, models, and deployed versions, can be linked and reproduced across its development, validation, and post-market phases. According to the EU AI Act, developers must maintain complete technical documentation that allows identification of any version of an AI system and its components, ensuring accountability, reproducibility, and transparency throughout the lifecycle [1] [2].

This aligns with global standards such as IEC 62304 and IMDRF SaMD guidance, which require configuration management and controlled change processes for software used in medical devices. Maintaining structured, versioned trace links between design inputs, model outputs, and field performance data supports regulatory compliance and patient safety.

Suggested core data to maintain

Each record should include: ID, creator, timestamp, unique hash, origin or lineage, storage location, linked requirements or risks, verification report, and release identifier.

Requirements: clinical or functional needs defined by the manufacturer, linked to design, implementation, and validation outputs [3] [4].

1. Risk controls: safety measures and mitigations with corresponding verification evidence and test results. [4] [5]
2. Dataset records: dataset name, provenance, preprocessing pipeline, label scheme, integrity checksum, and version reference [6] [7]
3. Training code and pipelines: repository commit, configuration files, and container image digest for the executed build [8]
4. Model versions: model ID, algorithm details, training dataset references, hyperparameter configurations, and evaluation results [6] [7] [9]
5. Validation reports: performance metrics, acceptance thresholds, and reviewer confirmation of pass or fail criteria [1] [10]
6. Released software versions: production versions including linked model IDs, validation artifacts, and approved change category [4] [10]
7. Operational monitoring data: in-service logs tied to model versions, identifying drift indicators and post-market actions [1] [9]

Suggested lifecycle management steps

1) Define unique identifiers and metadata schema consistent with quality system documentation [1][2]
2) Capture immutable hashes for all datasets, models, and containers and record links in a registry such as ML flow or DVC [6] [7]
3) Implement automated lineage capture in CI/CD pipelines connecting training runs to specific datasets and code commits [8]

4) Apply predefined change categories (PCCP) to classify and govern model updates, each with required validation actions [10]
5) Bundle and archive evidence for each release, including requirement and risk mappings, datasets, training runs, and reports [1] [4]
6) Conduct post-market performance monitoring, linking field results to model and dataset identifiers to support continuous improvement [1] [9]

8.1. Performance monitoring and post-market surveillance

Performance monitoring and post-market surveillance (PMS) for AI enabled medical devices require a lifecycle view of device safety and effectiveness. key components include defining meaningful performance metrics, establishing real-world data collection and analysis, detecting drift or degradation, adapting models responsibly, documenting changes and maintaining traceability.

AI enabled medical devices evolve over time and may degrade in performance under changing clinical, data or workflow conditions. one recent study found that the existing adverse event reporting system for approximately 950 ai/ml devices in the United States was “insufficient for properly assessing the safety and effectiveness” of those devices [11]. Another scoping review noted that available methods for monitoring clinical AI are sparse and heterogeneous [12].

From risk management perspective from latest ongoing draft ISO/DTS 24971-2:2025, performance monitoring and post-market surveillance for AI-enabled medical devices are closely tied to the manufacturer’s risk management plan, particularly after deployment. For machine learning medical devices (MLMD), risk management should include monitoring model performance and determining when updates or retraining are needed. In line with DTS 24971-2:2025 and ISO 14971, manufacturers must maintain a system for collecting and reviewing safety-related information, considering model autonomy, potential drift, user acceptance, and clinical usability.

Drift refers to gradual, unintended changes in performance that can reduce reliability. To manage this, post-production activities should include defined processes for retraining the model with new data and validating results using separate test data. Concept improvement may also be required, involving refinement of algorithms, features, or acceptance criteria to restore performance.

For continuously learning MLMD*, it is important to set clear monitoring and testing strategies to confirm that performance and safety standards remain met. Continued support after deployment can also be strengthened through regular collaboration between healthcare organizations and AI developers to review performance and plan updates.

* MLMD: medical device that utilizes machine learning (DTS 24971-2:2025)

Suggested key monitoring metrics and methods

- traditional diagnostic performance metrics (sensitivity, specificity, area under receiver operating characteristic curve) remain relevant but may not capture drift or context change [12].
- data distribution monitoring: tracking input feature shifts, population changes, model confidence and calibration.
- real-world outcome tracking: linking algorithm output to clinical outcomes, adverse events, user feedback.

- signal detection workflows: identifying trends of degraded performance, bias, unintended use, model failures [11].
- change management: necessary when software updates or model retraining are planned for example via a predetermined change control plan (pccp) [13].

8.2. Human oversight and control

Effective human oversight in AI enabled medical devices is essential for maintaining safety, reliability, and compliance. Clinicians benefit when AI systems are designed to allow meaningful interaction, points where decisions can be reviewed, questioned, or overridden. Structuring workflows to support human machine teaming can help distribute responsibilities clearly while retaining authority to intervene when necessary [14]. Practical measures might include integrating alert systems, override options, or clearly defined escalation paths within clinical software.

Trustworthy AI requires embedding oversight across the device lifecycle. From data collection and algorithm design to validation, testing, and post market monitoring, checkpoints that allow humans to verify outcomes enhance accountability and confidence [15] [16]. Providing transparency tools, such as explainable AI modules, enables clinicians to understand AI outputs and make informed interventions. Without clarity in AI decision making, human oversight risks being superficial, potentially reducing patient safety and confidence in the technology.

Human behavior, including tendencies like automation bias, can influence the effectiveness of oversight. Designing systems and workflows that nudge users to remain vigilant through training, feedback loops, and monitoring dashboards can help ensure interventions occur appropriately [17] The EU AI Act emphasizes that human oversight should be effective, proportionate, and timely [18], highlighting the need for ongoing review and mechanisms for intervention even as AI systems adapt. By integrating review checkpoints, logging interventions, and monitoring performance continuously, AI enabled devices can operate safely, transparently, and in alignment with regulatory expectations.

Beyond operational oversight, another key area requiring human involvement is the validation of AI-generated data used in regulatory and quality activities. Validation processes must ensure that data produced by AI systems are accurate, consistent, and compliant with applicable standards. Human experts play a critical role in reviewing and interpreting these outputs, particularly when multiple AI tools are used, each designed for a specific regulatory scope such as EU or US compliance. As global requirements often diverge or conflict, a single model covering all jurisdictions is rarely feasible. Expert oversight is therefore needed to reconcile differing outputs, address missing data, and integrate findings into a unified validation strategy that ensures the product remains safe, compliant, and ready for clinical use [19].

9. Stakeholder Readiness

9.1. SMEs vs. large enterprises: capability gaps

SMEs often face significant capability gaps compared with larger enterprises, particularly in regulatory expertise, data governance capacity, and AI safety engineering. Limited resources make it harder for SMEs to meet the parallel obligations of MDR/IVDR and the AI Act, including robust technical documentation, lifecycle monitoring, and evidence generation. Large

enterprises typically have more mature QMS structures, in-house regulatory teams, and access to higher-quality datasets, giving them a compliance and scalability advantage.

9.2. Sectoral readiness and maturity levels

Readiness across the health and diagnostics sectors remains uneven. Some manufacturers, hospitals, and laboratories have advanced digital infrastructures, interoperable data pipelines, and established quality and information-security management systems, enabling faster adoption of AI as required under the AI Act. Others still operate with limited digitization, fragmented data, or immature governance processes, creating barriers to validation, monitoring, and safe deployment of AI-enabled devices and diagnostics

9.3. Training and AI literacy requirements

Across all stakeholder groups—clinicians, regulators, manufacturers, labs, and notified bodies—there is a rising need for structured AI literacy and targeted training. Key competencies include understanding machine-learning principles, model limitations, bias risks, human oversight duties, data and pivacy protection rules, and the documentation requirements under MDR/IVDR and the AI Act. Building this capability is essential to ensure safe use, correct interpretation of AI outputs, and informed, accountable decision-making throughout the device lifecycle.

10. Appendices

10.1. Glossary of terms
10.2. Reference standards and frameworks

11. Definitions

11.1. Sensitive data

The GDPR considers the following categories of personal data as "sensitive" and subject to stricter processing rules:

- **Racial or ethnic origin:** Data that indicates a person's race or ethnicity.
- **Political opinions:** A person's political beliefs.
- **Religious or philosophical beliefs:** Data concerning a person's religious or philosophical views.
- **Trade union membership:** Information about a person's membership in a trade union.
- **Genetic data:** Data related to the inherited or acquired genetic characteristics of an individual.
- **Biometric data:** Data processed to identify a human being uniquely.
- **Health-related data:** Any information about a person's physical or mental health.
- **Sex life or sexual orientation:** Data concerning an individual's sex life or sexual orientation.

Annex I Analysis: required documentation elements

#	Requirement Statement (verbatim)	Suggested document title	Top 3 highly cited papers (quotes)	3 latest 2025 papers (quotes)	Existing regulatory documents (quotes)
1(a)	its intended purpose, the name of the provider and the version of the system reflecting its relation to previous versions	intended purpose / device description / version history	model cards provide a structured description of a model's intended use scope and limitations enabling transparency [20] the machine learning community currently has no standardized process for documenting datasets we propose that every dataset be accompanied with a datasheet [21]	the rise of artificial intelligence and data science across industries underscores the pressing need for effective management and governance of machine learning models [22] in this paper we cover approaches to systematically govern assess and quantify bias across the complete life cycle of machine learning models [23] drawing on 1178 safety and reliability papers we find that corporate ai research increasingly concentrates on pre deployment areas while attention to deployment stage issues such as model bias has waned [24]	the technical documentation shall contain its intended purpose the name of the provider and the version of the system reflecting its relation to previous versions (annex iv 1(a))
1(b)	how the ai system interacts with or can be used to interact with hardware or software including with other ai systems that are not part of the ai system itself where applicable	functional description / integration specification	model cards are short documents that provide benchmarked evaluation and disclose the context in which models are intended to be used [8] datasheets for datasets will facilitate better communication between dataset creators and dataset consumers and encourage the machine	model lake a new alternative for machine learning models management and governance [22] data and ai governance an approach to systematically govern assess and quantify bias across the complete life cycle of machine learning models [23] real world gaps in ai governance research [24].	the technical documentation shall contain how the ai system interacts with or can be used to interact with hardware or software including with other ai systems (annex iv 1(b))

			learning community to prioritise transparency and accountability [21]		
1(c)	the versions of relevant software or firmware and any requirements related to version updates	software / firmware version management	the machine learning community currently has no standardized process for documenting datasets [21] model cards provide a structured description enabling transparency [20].	model lake a new alternative for machine learning models management and governance [22] data and ai governance an approach to systematically govern assess and quantify bias across the complete life cycle of machine learning models [23] real world gaps in ai governance research [24]	the technical documentation shall contain the versions of relevant software or firmware and any requirements related to version updates (annex iv 1(c))
1(d)	the description of all the forms in which the AI system is placed on the market or put into service such as software packages embedded into hardware downloads or APIs	deployment forms specification	machine learning offers a fantastically powerful toolkit for building useful complex prediction systems quickly we find it is common to incur massive ongoing maintenance costs in real world ML systems [[21] model cards provide structured summaries of model intended use evaluation and limitations to improve transparency [20] datasheets for datasets include the dataset's intended use to guide proper application and reduce harm [21]	model lake enhanced model lifecycle management discovery audit and reusability [22] blueprints of trust AI system cards a living document provides a single accessible source of truth [6] local ai governance addressing model safety deployment becomes invisible [24].	the technical documentation shall contain the description of all the forms in which the AI system is placed on the market or put into service such as software packages embedded into hardware downloads or APIs (annex iv 1(d))
1(e)	the description of the hardware on which the AI system is intended to run	target hardware specification	understanding the purpose of each component is essential to prevent silent failures in ML systems [21] model cards	blueprints of trust integrating security and safety identifiers [23] rethinking ai governance introduces the gatekeeper	the technical documentation shall contain the description of the hardware on

			describe what the model does the tasks it performs and how outputs should be interpreted [20] datasheets document the dataset collection methods and hardware constraints so that performance claims are credible [21]	governance model [4] AI governance beyond 2025 UN pathways and implications [22]	which the AI system is intended to run (annex iv 1(e))
1(f)	where the AI system is a component of products photographs or illustrations showing external features the marking and internal layout of those products	product integration / visual documentation	documenting system architecture helps trace dependencies and identify failure points in complex ML systems [21] evaluation metrics should be documented to demonstrate expected performance and limitations [20] datasheets include detailed information on dataset provenance composition and collection process [21]	model lake for model lifecycle management audit and reuse [22] local ai governance open source models now run on personal computers deployment becomes invisible [24] AI Governance a framework for responsible and compliant artificial intelligence [23].	the technical documentation shall contain photographs or illustrations showing external features the marking and internal layout of those products (annex iv 1(f))
1(g)	a basic description of the user interface provided to the deployer	user interface overview	model cards provide a structured description of model enabling transparency and responsible deployment [20] we explore several ML specific risk factors including configuration issues [21] datasheets will facilitate better communication between dataset creators and dataset consumers and encourage the machine learning community to	blueprints of trust provides a comprehensive dynamic record of an AI system's security and safety posture [6] ai governance beyond 2025 UN pathways and implications [22] 2025 AI deployment and governance survey report [24].	the technical documentation shall contain a basic description of the user interface provided to the deployer (annex iv 1(g))

			prioritise transparency and accountability [21].		
1(h)	instructions for use for the deployer and a basic description of the user interface provided to the deployer where applicable	user manual / instructions for use	evaluation metrics should be documented to demonstrate expected performance and limitations [20] documenting data inputs must be fully documented to prevent silent failures caused by drift or bias [21] datasheets must capture the sources preprocessing and intended use to ensure reproducibility [21]	local ai governance deployment becomes invisible [4] model lake management and governance of machine learning models [22] ai governance a framework for responsible and compliant artificial intelligence [23].	the technical documentation shall contain instructions for use for the deployer and a basic description of the user interface provided to the deployer where applicable (annex iv 1(h))
2(a)	the methods and steps performed for the development of the AI system including where relevant recourse to pre-trained systems or tools provided by third parties and how those were used integrated or modified by the provider	development methodology / process documentation	machine learning offers a fantastically powerful toolkit for building useful complex prediction systems quickly we find it is common to incur massive ongoing maintenance costs in real-world ML systems [21] model cards provide a structured description of a model's intended use scope and limitations enabling transparency [20] we propose that every dataset be accompanied with a datasheet to encourage transparency and accountability [21].	inspired from research on data lakes we introduce the concept of model lakes we formalize key model lake tasks including model attribution versioning search and benchmarking [22] yprov4ml effortless provenance tracking for machine learning systems focuses on flexibility and extensibility enables users to integrate additional data collection tools via plugins [23] ai governance and frameworks how to manage summarizes frameworks and practical governance practices for lifecycle documentation and controls [24].	the technical documentation shall contain the methods and steps performed for the development of the AI system including recourse to pre-trained systems or tools provided by third parties and how those were used integrated or modified by the provider (annex iv 2(a))
2(b)	the design specifications of the system namely the general logic	design specification /	model cards provide structured summaries and disclose the	blueprints of trust ai system cards for end-to-end	the technical documentation shall

	of the AI system and of the algorithms the key design choices including the rationale and assumptions made including with regard to persons or groups of persons in respect of who the system is intended to be used the main classification choices what the system is designed to optimise for and the relevance of the different parameters the description of the expected output and output quality of the system the decisions about any possible trade-off made regarding the technical solutions adopted to comply with the requirements set out in chapter iii section 2	algorithm description / decision rationale	context in which models are intended to be used [20] hidden technical debt shows how implicit assumptions and design decisions create maintainability and safety risks [21] explainability literature stresses documenting assumptions and model objectives so stakeholders can assess fairness and limits [25]	transparency and governance introduces hazard-aware system card hasc framework to capture design choices and hazards [6] ai governance and frameworks how to manage emphasizes codifying design rationale and fairness assumptions into living documents [24] model lakes EDBT 2025 model attribution and metadata support explanation of design choices across large model collections [22].	contain the design specifications of the system namely the general logic key design choices expectations of output and output quality and trade-offs (annex iv 2(b))
2(c)	the description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing the computational resources used to develop train test and validate the AI system	system architecture / computational resources specification	a clear architecture diagram helps trace dependencies and identify failure points in complex ML systems [21] provenance and workflow literature emphasizes recording component interactions for reproducibility [25] model cards and system cards should include architecture and integration notes to support transparency [20]	yprov4ml effortless provenance tracking for machine learning systems collects provenance data in json format compliant with w3c prov [23] model lakes edbt 2025 model lakes formalize versioning attribution and architecture metadata for large model collections [22] blueprints of trust sep 2025 system cards capture end-to-end architecture and processing flows to aid governance [24].	the technical documentation shall contain the description of the system architecture explaining how software components build on or feed into each other computational resources used to develop train test and validate (annex iv 2(c))

2(d)	where relevant the data requirements in terms of datasheets describing the training methodologies and techniques and the training data sets used including a general description of these data sets information about their provenance scope and main characteristics how the data was obtained and selected labelling procedures data cleaning methodologies	training & data datasheets / data governance file	we propose that every dataset be accompanied with a datasheet to encourage transparency and accountability [21] documenting preprocessing steps is key to understanding model performance and avoiding hidden biases [25] tracking ml experiment metadata accelerates reproducibility and provides audit trails for datasets labels and transformations [26]	model lakes edbt 2025 model lakes include dataset pointers sampling metadata and provenance context [22] provenance tracking in large-scale machine learning provides json provenance compatible with w3c prov to record dataset lineage and transformations [23] provenance tracking for machine learning models a consolidated review and tooling overview for dataset and label provenance [24].	the technical documentation shall contain datasheets describing the training methodologies and techniques and the training data sets used provenance scope main characteristics how data was obtained and selected labelling procedures data cleaning methodologies (annex iv 2(d))
2(e)	assessment of the human oversight measures needed in accordance with article 14 including an assessment of the technical measures needed to facilitate the interpretation of the outputs of ai systems by the deployers in accordance with article 13(3) point (d)	human oversight assessment / interpretability controls	model cards should describe circumstances requiring human oversight and provide guidance for human usage [20] human-in-the-loop design and human factors research highlight how to structure oversight to avoid automation bias [25] automation bias and over-reliance are real risks document the human tasks and decision points explicitly [21].	blueprints of trust 2025 hazard-aware system cards include explicit human oversight guidance for deployers [6] taibom trustworthy ai systems 2025 recommend human oversight patterns and operator guidance as part of governance artifacts [24] IMDRF gmlp 2025 principles emphasize human role and multidisciplinary expertise across life cycle [27]	the technical documentation shall contain assessment of the human oversight measures needed and technical measures to facilitate interpretation of outputs (annex iv 2(e))
2(f)	where applicable a detailed description of pre-determined changes to the ai system and its performance together with all the relevant information related to the technical solutions adopted to ensure	predetermined change plan / pccp / continuous compliance plan	predetermined change control plans are mechanisms for safe controlled updates to learning systems [27] hidden technical debt highlights risks of unplanned changes and the need for documented change	predetermined change control plans PCCP guidance examples 2025 show how to document planned changes and performance acceptance criteria [24] PCCP Implementations and case studies 2025 show	if you plan to let the model change in production auditors want to see the guardrails what changes are allowed what tests are required and how

	continuous compliance of the ai system with the relevant requirements set out in chapter iii section 2		control [21] model lifecycle governance literature recommends predetermining retraining criteria and update controls [25]	templates for documenting pre-determined changes [6] model lakes model lake tooling 2025 supports versioning and controlled deployment workflows [22]	you'll ensure continued compliance produce a pccp or equivalent
2(g)	the validation and testing procedures used including information about the validation and testing data used and their main characteristics metrics used to measure accuracy robustness and compliance with other relevant requirements set out in chapter iii section 2 as well as potentially discriminatory impacts test logs and all test reports dated and signed by the responsible persons including with regard to pre-determined changes as referred to under point (f)	validation & test reports / test logs / signed evidence	evaluation metrics should be reported across relevant subgroups to show fairness and limitations [20] define metrics to measure system performance including accuracy drift and error rates [25] testing logging and signed reports are standard engineering controls to demonstrate verification [21].	2025 evaluation frameworks and practical guides describe reproducible validation pipelines and subgroup reporting [22] unsupervised shift detection and drift monitoring papers 2025 define monitoring metrics and validation approaches [23] PCCP & gmlp 2025 examples include test reporting templates and signatures for accountable release [27]	auditors will expect dated signed test logs not a slide deck provide test datasets metrics subgroup analyses and signed acceptance records for each release and for planned changes
2(h)	cybersecurity measures put in place	cybersecurity & resilience report	security vulnerabilities must be documented to prevent unauthorized access or manipulation [21] adversarial robustness and security research show the need for documented controls and mitigation strategies [25] privacy engineering and secure data practices should be	regulatory security guidance enisa ncsc 2025 updates emphasise documenting security controls and incident response [6] provenance tooling yprov4ml can integrate security-relevant events into provenance logs for audit [22] IMDRF GMLP 2025 good machine learning practice	document access control encryption integrity checks incident response and security testing if your ai is attacked or tampered with this report is how you prove you had defenses

			recorded as part of system documentation [28]	highlights security and quality controls across lifecycle [9]	
3	detailed information about the monitoring functioning and control of the AI system in particular with regard to its capabilities and limitations in performance including the degrees of accuracy for specific persons or groups of persons on which the system is intended to be used and the overall expected level of accuracy in relation to its intended purpose the foreseeable unintended outcomes and sources of risks to health and safety fundamental rights and discrimination in view of the intended purpose of the AI system the human oversight measures needed in accordance with article 14 including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the deployers specifications on input data as appropriate	monitoring functioning & control report / capabilities & limitations file	performance metrics must be reported across subgroups to show differential performance [20] concept drift literature stresses monitoring to detect degradation in performance for specific populations [25] hidden technical debt and system-level issues can cause unintended consequences document monitoring to catch these [21]	post-market monitoring and telemetry pipeline papers 2025 outline how to capture in-service metrics and subgroup accuracy [23] blueprints of trust 2025 recommends hazard-aware monitoring specifications aligned to system cards [24] MDCG EU medical guidance 2025 functional traceability and lifecycle logging are required for high-risk systems [27].	this section is the living monitoring plan show the metrics you'll track in service how you'll measure subgroup performance foresee harms and how humans will control or interpret outputs without it you have no safety net
4	a description of the appropriateness of the	performance metrics	choose metrics that reflect the real world task accuracy alone is often insufficient use	2025 evaluation frameworks provide guidance on metric selection and justification for	don't just list numbers justify why each metric is suitable for the claim

	performance metrics for the specific AI system	appropriateness justification	domain-relevant metrics [20] evaluation surveys recommend metrics for drift calibration and subgroup fairness [25] model reporting standards call for metric justification tied to intended use	regulatory evidence [22]IMDRF GLMP 2025 emphasize suitability of metrics for clinical claims [27] MDCG 2025 guidance clarifies metric appropriateness for health-sector AI [23]	you make and how it maps to clinical business outcomes and harms that's what assessors will check
5	a detailed description of the risk management system in accordance with article 9	risk management file article 9 compliance	ISO 14971 requires a documented risk management process for medical devices [29] risk management and safety engineering literature show ml-specific hazards require documented processes [25] hidden technical debt explains systemic risk accumulation if not managed [21]	imdrf gmlp 2025 gives lifecycle risk management principles for ai ml medical devices [27] MDCG and EU guidance 2025 highlight functional traceability and lifecycle logging to support risk management [23] PCCP GMLP examples 2025 demonstrate risk acceptance and monitoring implementation [24].	show hazard logs severity likelihood assessments mitigations residual risk acceptance and traceability to design controls this is the core safety dossier
6	a description of relevant changes made by the provider to the system through its lifecycle	change history / version & release notes	version control and change logs are essential to reproduce experiments and audit systems [8] hidden technical debt unknown changes cause failures unless change management exists [21] model registries and change logs are part of good mlops practice [25]	model lakes 2025 and provenance tools document version graphs and change histories [22] 2025 supports recording change events for reproducibility [23] IMDRF FDA 2025 guidance references change controls for lifecycle compliance [27].	keep a clear release log who changed what why and the test evidence regulators will read this to ensure no unapproved or uncontrolled changes occurred
7	a list of the harmonised standards applied in full or in part the references of which have been published in the official journal of the european	standards & conformance matrix	standards mapping is standard practice in regulated device submissions to demonstrate conformity [29] guidance texts recommend documenting	MDCG 2025-6 and other eu guidance list applicable standards and how to declare conformity [23] IMDRF documents and FDA gmlp	create a clean table each annex iv requirement applied standard or technical solution

	union where no such harmonised standards have been applied a detailed description of the solutions adopted to meet the requirements set out in chapter iii section 2 including a list of other relevant standards and technical specifications applied		harmonized standards and alternate technical solutions where standards are not applicable [25] mapping to standards reduces assessor uncertainty and speeds certification [21].	provide links to applicable standards for medical ai [9] annual ai governance reports itu 2025 list candidate harmonized standards in practice [24]	rationale that is how you prove conformity
8	a copy of the eu declaration of conformity referred to in article 47	eu declaration of conformity doc copy	—	—	the technical documentation shall contain a copy of the EU declaration of conformity (annex iv 8)
9	a detailed description of the system in place to evaluate the ai system performance in the post-market phase in accordance with article 72 including the post-market monitoring plan referred to in article 72(3)	post-market monitoring plan & evaluation system	continuous monitoring of data and model performance is critical to detect and mitigate drift [25] production monitoring patterns and telemetry capture are necessary for reliable in-service operation [28] post-market evaluation bridges the gap between pre-market validation and in-service behaviour [21].	post-market monitoring an important ai act requirement 2025 article 72 requires a post-marketing ai monitoring system proportionate to risk collect usage data assess compliance trigger actions [23] MDCG 2025-6 interplay between mdr and ai act article 12 mandates that high-risk ai systems maintain logs of system performance and behaviour throughout their lifecycle [27] PCCP GMLP materials 2025 provide examples of monitoring metrics and retraining triggers [24].	this is the operational promise how you'll continuously measure detect deterioration log incidents and take corrective action it's crucial to keep the system safe after deployment regulators will read this carefully

Annex II References

[1] U. F. a. D. Administration, Good Machine Learning Practice (GMLP) and AI Guidance, FDA, 2025.

[2] E. Union, EU Artificial Intelligence Act; Articles 9 and 11 technical documentation and record keeping, 2024.

[3] B. Ramesh and M. Jarke, Toward Reference Models for Requirements Traceability, IEEE, 2001.

[4] I. TC62, Medical device software — Software life cycle processes, IEC / ISO, 2006.

[5] F. e. al., Regulatory Challenges Across the Life Cycle of AI Medical Devices, 2025 .

[6] I. e. al, Machine Learning Experiment Management Tools Review, 2024.

[7] K. e. al., AI Model Passport (AIPassport), 2025.

[8] Martina, DevOps Approaches for Medical Device Software Maintenance, 2024.

[9] d. A. e. al., Medical Machine Learning Operations Framework, 2025.

[10] C. e. al., Predetermined Change Control Plans for AI ML SaMD, 2025 .

[11] B. et al., A general framework for governing marketed AI/ML medical devices. npj Digital Medicine., 2025.

[12] Andersen E.S, Monitoring performance of clinical artificial intelligence in health care: a scoping review. JBI Evidence Synthesis., 2024.

[13] U. F. a. D. Administration, Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence Enabled Device Software Functions. Guidance, 2024.

[14] L. F. &. M. T. Andreas Tsamados, Human control of AI systems: from supervision to teaming, Springer Open, 2024..

[15] J. Z. &. Z.-m. Zhang, Ethics and governance of trustworthy medical artificial intelligence, Springer , 2023.

[16] F. D. Health, A trustworthy AI reality-check: the lack of transparency of artificial intelligence products in healthcare., Frontiers Digital Health, 2024..

[17] .. European Journal of Risk Regulation, Automation Bias in the AI Act: On the Legal Implications of Attempting to De-Bias Human Oversight of AI,, 2025.

[18] S. W. ,. B. M. Daria Onitiu, How AI challenges the medical device regulation: patient safety, benefits, and intended uses., Journal of Law & Biosciences, 2024.

[19] E. Union, MDCG 2025-6: Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA), 2025.

[20] M. e. a. Mitchell, Model Cards for Model Reporting., 2019.

[21] D. e. a. Sculley, Hidden Technical Debt in Machine Learning Systems, 2015.

[22] S. e. a. Garouani, Model Lake: Enhanced Model Lifecycle Management, EDBT, EDBT, 2025.

[23] M. e. a. Sidhpurwala, Blueprints of Trust: AI System Cards for End-to-End Transparency, 2025.

[24] B. Sokhansanj, Local AI Governance: Addressing Model Safety,, 2025.

[25] S. e. a. Schelter, Provenance and Reproducibility in ML Systems, 2017.

[26] J. e. a. Gama, Post-Market Evaluation and Monitoring of AI Systems, 2019–2024.

[27] IMDRF, Good Machine Learning Practice (GMLP) Guidance, 2025.

[28] J. e. a. Gama, Post-Market Evaluation and Monitoring of AI Systems,, 2019–2024.

[29] ISO, Medical devices — Application of risk management to medical devices, ISO, 2019.