

NAVIGATING THE EU AI ACT 2024/1689: A PRACTICAL COMPLIANCE PLAYBOOK FOR AI-ENABLED MEDICAL DEVICES (AIMD)

Decoding the EU AI Act and its Implications
on AI-Enabled Medical Devices



CONTENTS

Abstract	03
Introduction to EU AI Act – 2024/1689	03
Key Definitions	05
Purpose of EU AI Act-2024/1689	06
EU AI Act – 2024/1689 – Scope and Out of Scope	07
Prohibited AI Practices & AI Literacy Requirements	08
EU AI Act – 2024/1689 STRUCTURE	09
Content of Technical Documentation as per EU AI Act-2024/1689	10
Risk-Based Classification Approach	11
Recognized Standards	12
EU AI Act Implementation Timeline	14
Use of AI in Healthcare	15
Possible Challenges that Deployers/Manufacturers/Providers of AI for Medical Purpose Might Face	16
Conformity Assessment Strategy for AI enabled Medical Device	17
Compliance Checklist for Deployers/ Manufacturers / Providers for General Purpose AI Systems and High-Risk AI Systems	18
Conclusion	19
About the Author	19
About Cyient	20

Abstract

The European Union Artificial Intelligence Act (EU AIA – 2024/1689) marks a significant regulatory milestone in the global governance of AI. Focused on fostering safe, trustworthy, and human-centric AI systems, it sets out a harmonized legal framework applicable across sectors, with particular implications for healthcare and medical device industries.

This whitepaper provides a practical guide for deployers, manufacturers, and providers of AI-enabled medical devices (AIMDs)—to understand, prepare for, and comply with the Act. It decodes the regulation's intent, structure, and scope while outlining compliance obligations such as risk classification, documentation requirements, conformity assessments, and AI literacy.

With healthcare at the forefront of AI innovation, this document offers actionable insights to navigate the evolving regulatory landscape while promoting responsible AI use that aligns with ethical and safety standards.

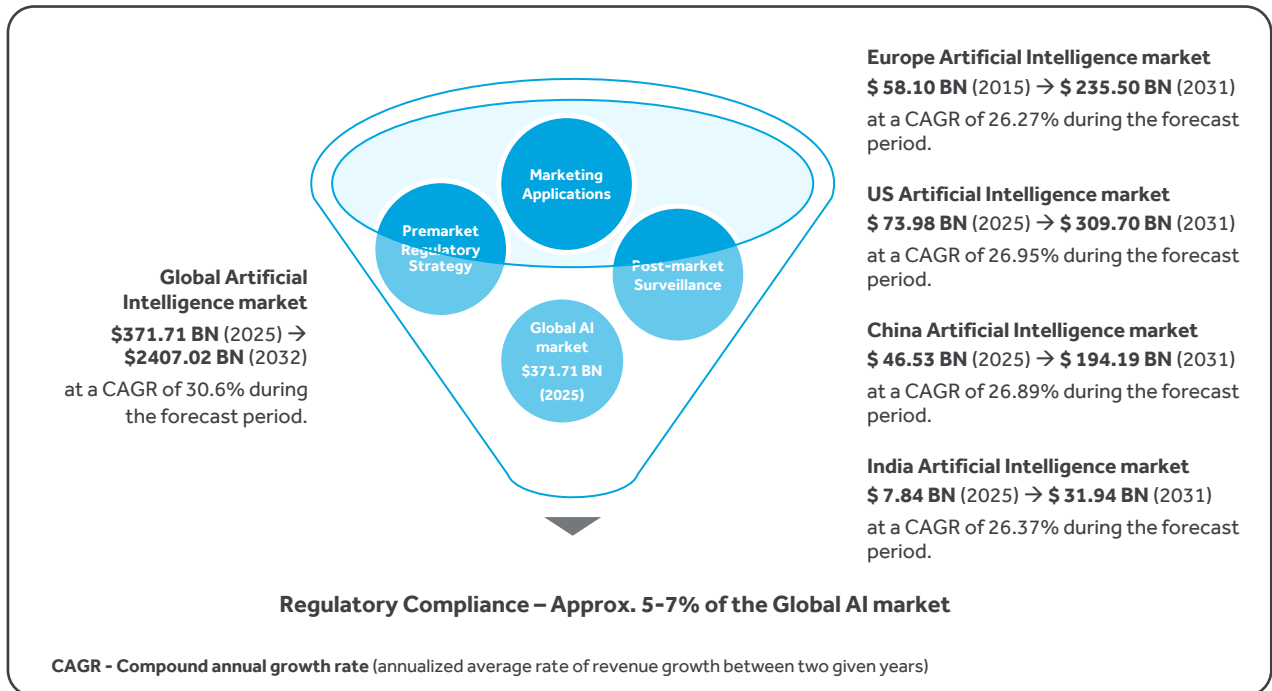
Introduction to the EU AI Act

Artificial intelligence (AI) presents immense opportunities across healthcare—from accelerating diagnostics to enhancing treatment accuracy. Yet, its complexity introduces risks to safety, privacy, and fundamental rights. The EU AI Act provides a structured framework to harness AI's benefits while mitigating its risks through a risk-based regulatory approach. Key objectives include:

- **Building Trustworthy AI:** Embedding requirements that ensure AI systems respect fundamental rights and are safe, transparent, and explainable.
- **Risk-Based Regulation:** Implementing a tiered framework that imposes stricter obligations on high-risk AI systems—especially those that impact health, safety, or fundamental freedoms.
- **Mandatory Compliance Measures:** Introducing conformity assessment procedures, post-market monitoring, and human oversight requirements for high-risk applications.
- **Enhancing Transparency:** Requiring clear disclosures for AI systems like chatbots and synthetic content (e.g., deepfakes), to inform users when they're interacting with AI.
- **Strengthening Governance:** Enforcing rules through national competent authorities supported by a coordinated governance mechanism at the EU level.
- **Fostering Responsible Innovation:** Promoting AI innovation through mechanisms like regulatory sandboxes and targeted support for startups and SMEs.



Artificial Intelligence – Global Market Share



Statista - The Statistics Portal for Market Data, Market Research and Market Studies
Artificial Intelligence Market Size & Trends, Growth Analysis, Forecast [2032]



Key Definitions

AI System



A machine-based system capable of autonomy and adaptiveness after deployment, producing outcomes such as predictions, recommendations, or decisions.

Substantial Modification



A post-market change to an AI system that was not anticipated during the original conformity assessment. Such changes affect the system's compliance with high-risk AI requirements or alter its originally intended purpose.

AI Regulatory Sandbox



A supervised framework established by a competent authority that allows AI providers to develop, train, validate and test innovative AI systems—often in real-world conditions—within a controlled, time-bound regulatory environment.

AI Literacy



The combination of skills, knowledge and understanding required by providers, deployers and impacted individuals to responsibly engage with AI systems. This includes awareness of AI's benefits, limitations, and associated risks.

Biometric Identification



The automated process of recognizing individuals physical, physiological, behavioral, or psychological traits by comparing biometric data against stored datasets to verify identity.

Emotion Recognition System



An AI system designed to detect or infer the emotional states or intentions of individuals based on their biometric inputs.

AI Office



A European Commission body tasked with implementing, monitoring, and supervising the governance of AI systems and general-purpose AI models. References to the "AI Office" in the regulation refer to this central authority.

Systemic Risk



Risks stemming from powerful general-purpose AI models with wide-reaching impact—such as threats to public health, safety, rights, or societal structures—that can cascade across sectors or markets.

Downstream provider



Any entity that integrates an AI model into its system—whether self-developed or sourced through partnerships—thus contributing to the deployment and operation of the final AI solution.

Purpose of EU AI Act – 2024/1689

The Act aims to regulate AI in a manner consistent with European Union values, with the following core objectives:



Scope: The Regulation Applies To	Out of Scope: The Regulation Does Not Apply To
Providers placing AI systems or general-purpose AI models on the EU market—regardless of where they are established	Areas outside the scope of Union law, including matters of national security
Deployers of AI systems established or operating within the EU	AI systems used exclusively for military, defense, or national security purposes
Non-EU providers and deployers where AI output is used within the EU	AI systems not placed on the market, but whose output is used in the EU for military/national security
Importers and distributors of AI systems	Public authorities in third countries or international organizations involved in law enforcement cooperation, where adequate safeguards exist
Manufacturers placing AI systems integrated within their products on the market under their name	Provisions under Regulation (EU) 2022/2065 concerning intermediary service liability
Authorized representatives of non-EU providers	AI systems or models developed and used solely for scientific R&D
Affected persons located within the EU	GDPR, ePrivacy Directive, and criminal justice data protection regulations still apply (Regulations (EU) 2016/679, 2018/1725, 2002/58/EC, 2016/680)
High-risk AI systems as per Article 6(1), limited to Articles 102–109 and 112, plus Article 57 only when harmonized rules apply	Pre-market research, testing, or development of AI systems before placement on the market (unless conducted in real-world conditions)
Data protection, privacy, and confidentiality obligations under EU law remain applicable	Consumer protection and product safety rules under other EU legislation remain unaffected
	Natural persons using AI systems for purely personal, non-professional purposes
	Laws or agreements offering greater protection for workers' rights than the EU AI Act provisions
	AI systems under open-source licenses, unless they fall under high-risk or prohibited categories (Article 5 or 50)

Prohibited AI Practices & AI Literacy Requirements

The EU AI Act explicitly bans certain AI applications deemed to pose unacceptable risks:

Prohibited AI Practices

Manipulative AI: Use of subliminal or deceptive techniques that distort user behavior and cause harm is prohibited.

Exploitation of Vulnerabilities: AI systems must not exploit individuals based on age, disability, or socioeconomic status.

Social Scoring: Systems that generate social scores leading to unfair or discriminatory treatment are banned.

Predictive Policing: AI cannot be used to predict criminal behavior based solely based on profiling or personality traits.

Facial Recognition Databases: Creating facial recognition databases by scraping images from the internet without consent is forbidden.

Emotion Recognition in Work/Education: Emotion recognition systems are not allowed in workplaces or educational institutions, except in cases related to medical or safety reasons.

AI literacy requirements

Providers and deployers of AI systems are required to:

- Take all reasonable measures to ensure sufficient AI literacy among staff and individuals involved in operating or using the AI systems.
- Consider the users' technical knowledge, experience, education, and training.
- Account for the specific context and the individuals or groups the AI system will impact.

Biometric Categorization: AI systems must not categorize individuals based on race, political opinion, religion, sexual orientation, etc., using biometric data.

"Real-Time" Remote Biometric Identification: Use in public spaces for law enforcement is permitted only under specific conditions, such as for serious threats (e.g., terrorism or abduction), and requires judicial authorization.

Safeguards and Conditions: The deployment of real-time biometric identification must be necessary, proportionate, and subject to strict safeguards. These include conducting impact assessments and maintaining formal registration processes.

National Laws: EU Member States may implement stricter national laws regulating biometric identification.

Reporting and Oversight: Member States must report on the usage of real-time biometric identification. The European Commission will publish annual reports, excluding sensitive data.



EU AI Act – 2024/1689 Structure

EU AI Act is organized into 13 Chapters and 13 Annexes, comprising a total of 113 Articles. The structure outlines the regulatory scope, obligations, governance mechanisms, and supporting documentation.

Articles	Key Subject Area
Articles 1 - 4	General Provisions: Subject matter, scope, definitions, and AI literacy
Article 5	Prohibited AI Practices
Articles 6 - 49	High-Risk AI Systems: Classification, requirements, provider and deployer obligations, conformity assessments
Articles 51 - 56	General-Purpose AI Models: Classification, provider obligations, codes of practice
Articles 57 - 63	Regulatory Sandboxes and Innovation Support: Real-world testing, SME support
Articles 64 - 71	Governance: AI Office, European AI Board, national authorities
Articles 62 - 94	Market Surveillance, Enforcement and Monitoring: Reporting and compliance controls
Articles 95 - 113	Final Provisions: Penalties, delegation, committee procedures, amendments, entry into force

Annexes Overview

Annex	Key Subject Area
Annex I	Union harmonization legislation list
Annex II	Criminal offences referred to in Article 5(1)(h)(iii)
Annex III	High-risk AI systems as per Article 6(2)
Annex IV	Technical documentation under Article 11(1)
Annex V	EU declaration of Conformity template
Annex VI	Conformity assessment: internal control
Annex VII	Conformity assessment: quality management system and technical documentation
Annex VIII	Registration information for high-risk AI systems (Article 49)
Annex IX	Real-world testing registration (Article 60)
Annex X	Legislative acts on large-scale IT systems in freedom, security and justice sectors
Annex XI	Technical documentation for general-purpose AI model providers (Article 53(1) (a))
Annex XII	Transparency information for downstream providers (Article 53(1), (b))
Annex XIII	Systemic risk designation criteria (Article 51)

Content of Technical Documentation as per EU AI Act

The technical documentation for an AI system must include, at a minimum, the following details, tailored to the system's characteristics and intended purpose.:

Section 1 - General description of AI system

- Intended purpose and provider name
- Interaction with other AI systems
- Versions of relevant software or firmware
- All forms in which the AI system is placed on the market or put into service
- Description of the hardware on which the AI system is intended to run
- If part of a product: visuals showing external features, markings, and internal layout Basic description of the user-interface provided to the deployer
- Instructions for use, wherever applicable

Section 2 - System Development and Architecture Methods and steps followed during development

- Design specifications, including overall logic and algorithms structures
- Description of system architecture, detailing software components interactions

- Data requirements, including datasheets and descriptions of training methodologies and data sets
- Human oversight measures and technical tools for output interpretability
- Pre-determined changes to system performance and technical solutions for ongoing compliance
- Validation, testing procedures, and cybersecurity measures implemented

Section 3 - Monitoring, Functioning and Control

- System performance capabilities and limitations
- Foreseeable unintended outcomes and risks to health, safety, fundamental rights or potential for discrimination
- Human oversight needs and corresponding technical measures
- Specifications on input data (as appropriate)



Section 4 - Performance Metrics

- Evaluation of the appropriateness and relevance of selected performance metrics

Section 5 - Risk Management System

- Detailed description of the system for identifying, assessing, and mitigating risks

Section 6 – Lifecycle Changes

- Documentation of relevant system updates or modifications made post-deployment

Section 7 - Standards and Compliance Solutions

- List of the harmonised standards applied and /or detailed descriptions of alternative compliance solutions

Section 8 - EU declaration of conformity

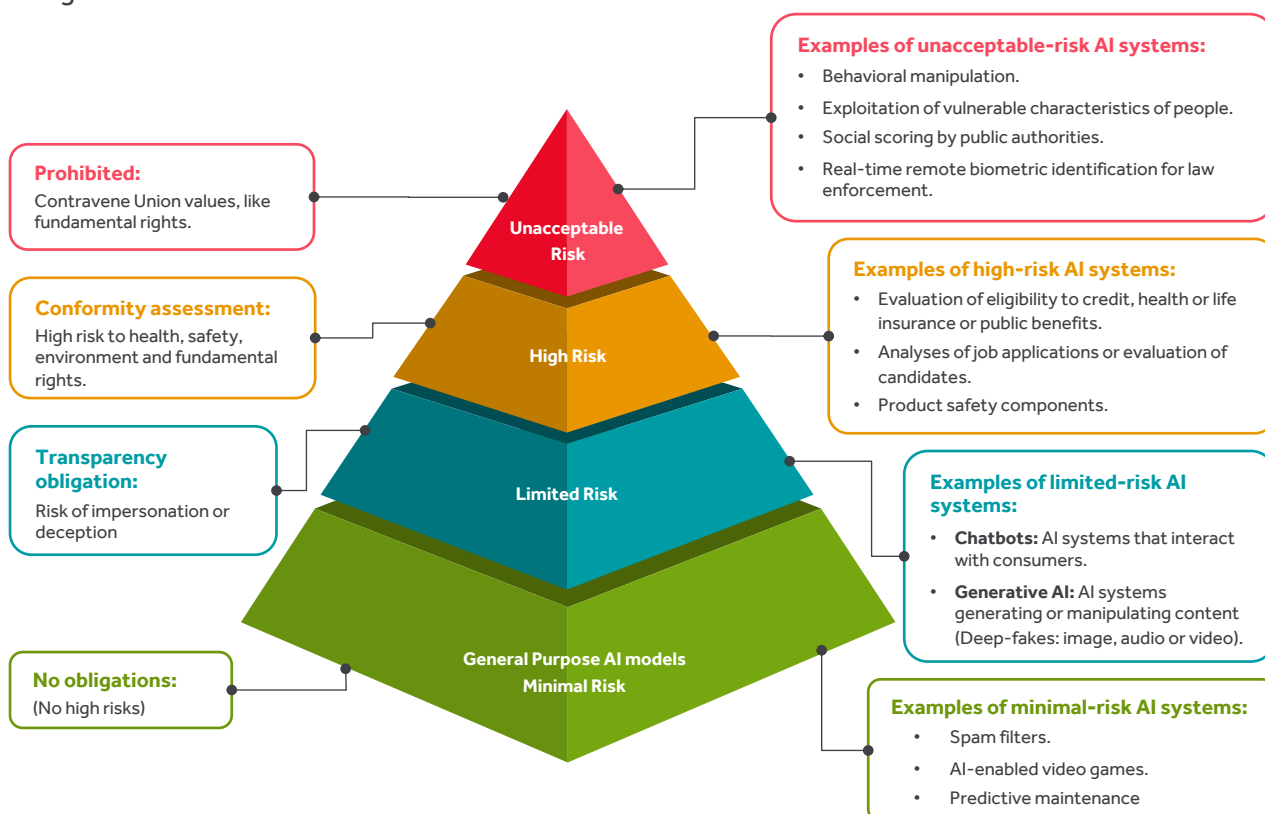
- Copy of the declaration

Section 9 - Post-Market Performance Monitoring

- Description of systems for ongoing evaluation
- Post-market monitoring plan

Risk-Based Classification Approach as per EU AI Act – 2024/1689

The EU AI Act classifies AI systems into four primary risk categories, with corresponding regulatory obligations:



Recognized Standards for AI-Enabled Medical Devices

The EU AI Act references several international and emerging standards to ensure safety, transparency, and robustness in AI-enabled systems—especially in regulated sectors like healthcare. These standards support compliance efforts for manufacturers, deployers, and providers of AI-enabled medical devices (AIMDs).

Selected Released Standards

Standard	Description	Status
ISO/IEC 24029-2:2023	Assessment of neural network robustness – Part 2: Methodology using formal methods	Released
ISO/IEC 8183:2023	AI – Data life cycle framework	Released
ISO/IEC 25059:2023	SQuaRE – Quality model for AI systems	Released
ISO/IEC TR 24368:2022	Overview of ethical and societal concerns	Released
ISO/IEC TR 24029-1:2021	Assessment of neural network robustness – Part 1: Overview	Released
ISO/IEC TS 4213:2022	Assessment of machine learning classification performance	Released
ISO/IEC 23894:2023	AI – Guidance on risk management	Released

Standards Under Development

Standard	Description	Stage
ISO/IEC CD 42005	AI system impact assessment	Committee
ISO/IEC CD 5259-5	Data quality governance for analytics and ML	Committee
ISO/IEC CD TS 8200	Controllability of automated AI systems	Committee
ISO/IEC CD TR 17903	Overview of machine learning computing devices	Committee
ISO/IEC CD TS 6254	Explainability of ML models and AI systems	Committee

Additional Relevant Standards

- IEEE 7001-2021 – Transparency of autonomous systems
- IEEE 7003-2022 – Algorithmic bias considerations
- ISO/IEC TR 24027 – Bias in AI systems and mitigation strategies
- ISO/IEC 29100 – Privacy framework
- IEC 81001-5-1 – Cybersecurity in health software lifecycle
- ISO/IEC 27001 / 27017 – Information and cloud security
- ISO/TS 82304-2 – Health apps – quality and reliability
- ISO/IEC 22989 / 23053 – Concepts, terminology, and AI system lifecycle
- ISO/IEC 23894 (Draft) – Risk management for AI
- ISO/IEC 42001 – AI Management System (AIMS)
- ISO/IEC TR 24028 – Trustworthiness in AI
- ISO/IEC 20546 – Big data overview

Medical Device-Specific Standards

- ISO 13485 – Quality management for medical devices
- ISO 14971 – Risk management for medical devices
- IEC 62304 – Software lifecycle processes
- IEC 60601-1 – Safety of electrical medical equipment

These standards play a key role in aligning AIMDs with both EU MDR/IVDR and the AI Act.

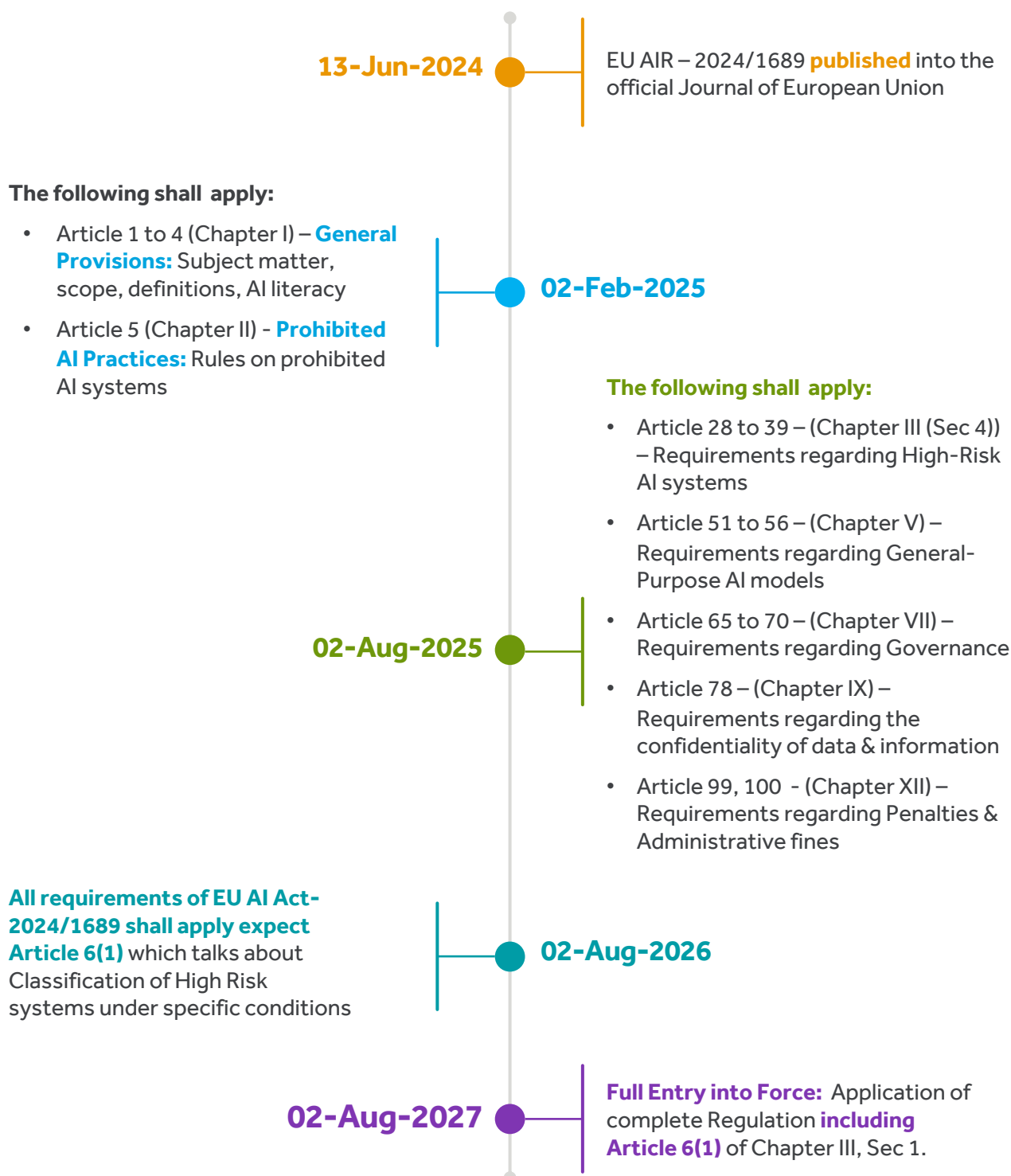
<https://www.bartolozzi.it/medical-device-ai/>

<https://eprints.dkit.ie/id/eprint/892/1/My1stPaper.pdf>



EU AI Act Implementation Timeline

The implementation of the EU AI Act follows a phased timeline to ensure stakeholders have sufficient time to adapt and comply. Below is a general overview based on the regulation's staged rollout:



Use of AI in Healthcare

AI is rapidly transforming the healthcare industry by enhancing diagnostic accuracy, optimizing treatment plans, streamlining workflows, and improving patient outcomes. Here are some of the major use cases of AI in healthcare, categorized by domain:



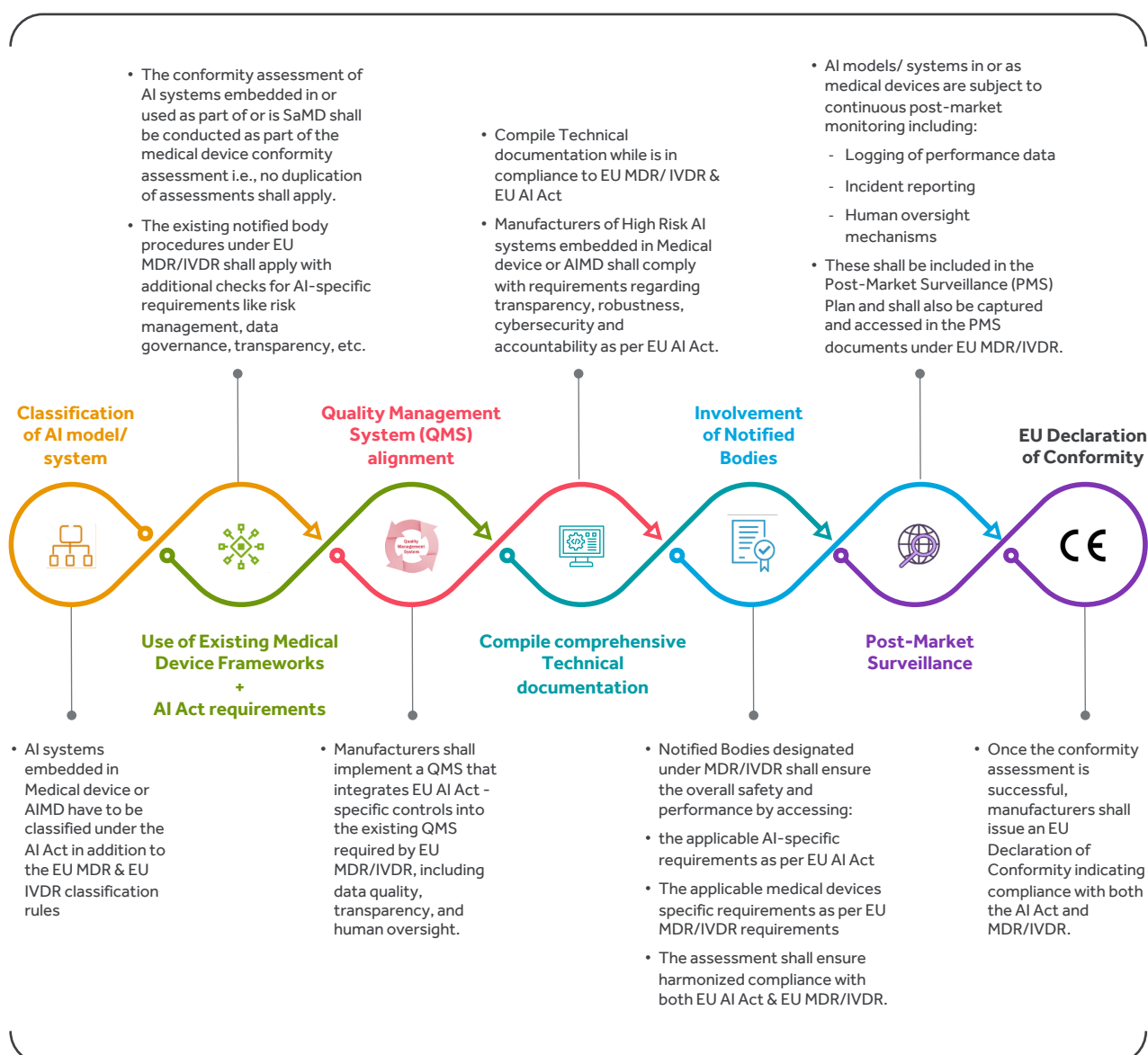
Possible Challenges that Deployers/Manufacturers/Providers of AI for Medical Purpose Might Face

Integrating AI into medical devices presents complex compliance challenges, particularly due to the dual regulatory landscape governed by the EU AI Act-2024/1689, and the EU MDR-2017/745 or EU IVDR-2017/746. The intersection of AI functionality and medical safety introduces both technical and procedural hurdles.

Dual Regulatory Burden	High Risk AI classification	Data Governance & Quality	Transparency & Explainability	Human Oversight	Robustness, Accuracy & Cybersecurity
- Manufacturers must comply with both the EU MDR/IVDR and EU AI Act. - Requires harmonization of conformity assessments technical documentation and quality system across two frameworks. - Potential for duplicated or conflicting requirements.	AIMD classified as High Risk as per EU AI Act shall comply stringent requirements such as human oversight, transparency, robustness and post-market monitoring	- Ensuring training and test data are: Relevant, representative, free of bias, Statistically appropriate, Collected lawfully under GDPR Challenge: Medical AI often uses retrospective, non-standardized, or anonymized datasets with quality or bias issues.	- AI outputs must be understandable to the intended user (e.g., physicians). - Difficult for complex models like deep learning or black-box AI to meet these criteria. - Manufacturers may need to redesign interfaces or limit the use of opaque algorithms.	- Manufacturers must ensure that human operators can understand, intervene, or override the AI system. - Manufacturer must have explicit design features, documentation, and training materials to enable human oversight.	- AI systems must maintain accuracy and performance throughout their lifecycle. - Real-world data often differs from training environments, impacting performance. - Cybersecurity risks increase with connected AI-enabled medical devices (e.g., remote updates, API access).
Continuous Learning & Software Updates	Technical Documentation & Traceability	Post-Market Monitoring	Notified Body Expertise Gaps	Ethical and Fundamental Rights Compliance	Cost & Time of Compliance
- Many AI systems are adaptive or continuously learning, which conflicts with the static certification model under EU MDR and the EU AI Act. Challenge: Validation & monitoring of that changes post-deployment.	- Manufacturers must produce detailed documentation about: - Model architecture - Training/testing data - Risk management - Logging and traceability mechanisms - These are not always readily available for third-party or open-source AI components.	- Requires active surveillance of AI model performance, bias, and safety over time. - Need for data pipelines, feedback loops, and incident reporting mechanisms tailored to AI.	- Many Notified Bodies lack AI-specific expertise. - Manufacturers may face delays or inconsistencies in conformity assessment procedures. - Ongoing need for capacity building among conformity assessment entities.	AI must respect human dignity, privacy, non-discrimination, and autonomy (restricted from AI prohibited practices as per EU AI Act). In case of High-Risk AI model/ system it becomes complicated to demonstrate the above features for the AI involved in life-and-death decisions, triage, or behavior prediction.	- Compliance adds substantial regulatory, engineering, and legal costs. - Small or medium manufacturers may find this particularly resource-intensive.

Conformity Assessment Strategy for AI-enabled Medical Device (AIMD)

When an AI system is integrated into a medical device or constitutes a standalone AI-enabled medical device, the conformity assessment process is not handled separately under the EU AI Act. Instead, it is embedded within the existing regulatory pathway defined by the EU Medical Device Regulation (MDR 2017/745) or In Vitro Diagnostic Regulation (IVDR 2017/746).



Compliance Checklist for Deployers, Manufacturers, and Providers of General-Purpose, and High-Risk AI systems



Determine Scope & Classification

- Is the product a medical device under EU MDR-2017/745 or EU IVDR-2017/746
- Does the device use AI for decision-making, diagnosis, or monitoring?
- If yes, classify it as a high-risk AI system under AI Act Article 6 + Annex II.



Conformity Assessment Route

- Choose the appropriate conformity assessment route under MDR/IVDR (e.g., Annex IX, X, XI).
- Ensure that this route includes AI-specific checks as per AI Act Article 24(3) and Article 43.



Quality Management System (QMS)

- Ensure that the QMS compliant to EU MDR-2017/745 or EU IVDR-2017/746
- Extend the QMS to meet EU AI Act Article 17, covering:
 - Lifecycle management of AI system
 - Data quality and governance
 - Logging and traceability
 - Post-market monitoring specific to AI



Technical Documentation

- Prepare comprehensive technical documentation (AI Act Art. 11 + EU MDR/IVDR Annex II& Annex III).
- Include AI-specific requirements such as:
 - Model architecture, training data, validation results
 - Risk analysis related to algorithmic failure
 - Human oversight mechanisms
 - Logging capability



Essential AI Requirements

- Ensure compliance with the following AI-specific obligations:
 - Risk management system (Art. 9)
 - Training and test data governance (Art. 10)
 - Automatic logging (Art. 12)
 - Transparency & accountability (Art. 13)
 - Human oversight mechanisms (Art. 14)
 - Accuracy, robustness, and cybersecurity (Art. 15)



Post-Market Monitoring & Reporting

- Draft a Post-Market Surveillance (PMS) plan under EU MDR/IVDR.
- Include AI-specific PMS elements as per AI Act Art. 19 –20:
 - Model performance over time
 - Unintended outputs
 - Incident reporting under both EU MDR/ IVDR and EU AI Act rules



EU Declaration of Conformity & CE Marking

- Draft Declare Conformity in accordance with EU MDR/IVDR + AI Act (Article 48).

Conclusion

The EU AI Act (2024/1689) marks a transformative step in establishing a robust and harmonized robust regulatory framework for artificial intelligence across the European Union. For the healthcare sector particularly medical device manufacturers integrating AI, this regulation introduces not only new compliance obligations but also opportunities to drive innovation within a well-defined legal and ethical structure.

By adopting a risk-based approach, the Act ensures that AI systems, especially those used in critical sectors like healthcare, are subject to appropriate oversight and accountability. It mandates transparent, safe, and human-centric AI while promoting public trust and technological progress.

To meet these evolving expectations, manufacturers, developers, and deployers of AI systems must align their internal processes with both existing medical device regulations (e.g., EU MDR/IVDR) and AI-specific obligations under this new law.

Proactive compliance will involve:

- Integrating regulatory requirements early in the design and development phase
- Investing in technical documentation and risk governance
- Leveraging recognized standards to establish traceability and conformity
- Promoting AI literacy and human oversight across all operational levels

Ultimately, the EU AI Act not only safeguards individuals but also lays the foundation for sustainable and responsible digital health innovation, supporting the ethical use of AI while enabling Europe to lead in the global AI landscape.

About the Author



Abhishek Kumar is a Subject Matter Expert in Medical Device Regulatory and Quality Assurance with over 14 years of experience. He has led the EU MDR 2017/745 sustenance program, managed multiple global engagements for top medical device companies, and supported the gap assessment, remediation, and submission of 70+ technical documents across EU MDR, ASEAN MDD, NMPA (China), Taiwan, and 10+ 510(k) submissions. He has authored 40+ Clinical Evaluation Reports (CERs) for Class I–III devices in line with MEDDEV 2.7.1 Rev-4 and developed proposals for market access in the U.S., Europe, and APAC (including ASEAN, China, Taiwan, and Japan). He also prepared and implemented regulatory plans for new product development across 90+ countries through feasibility analysis and cross-functional coordination.

About Cyient

Cyient (Estd: 1991, NSE: CYIENT) delivers intelligent engineering solutions across products, plants, and networks for over 300 global customers, including 30% of the top 100 global innovators. As a company, Cyient is committed to designing a culturally inclusive, socially responsible, and environmentally sustainable tomorrow together with our stakeholders.

For more information, please visit
www.cyient.com



Contact Us

North America Headquarters

Cyient, Inc.
99 East River Drive
5th Floor
East Hartford, CT 06108
USA
T: +1 860 528 5430
F: +1 860 528 5873

Europe, Middle East, and Africa Headquarters

Cyient Europe Limited
Apex, Forbury Road,
Reading
RG1 1AX
UK
T: +44 118 3043720

Asia Pacific Headquarters

Cyient Limited
L14, 333, Collins Street
Melbourne, Victoria, 3000
Australia
T: +61 4 7026 3817
F: +61 3 8601 1180

Global Headquarters

Cyient Limited
Plot No. 11
Software Units Layout
Infocity, Madhapur
Hyderabad - 500081
India
T: +91 40 6764 1000
F: +91 40 2311 0352

Follow us on:  