Emerging European Regulatory Trends for AI/ML Medical Devices

- Integrating QMS and Cyber Security

Track 5

Jens Lauber
Global Lead Quality & Regulatory Services, Medical Devices, Accenture

Introduction to the EU AI Act

Top 6 keywords you need to know about the EU AI Act

The **EU AI Act** is the first comprehensive legal framework designed to regulate artificial intelligence across Europe. Its primary goal is to ensure that AI is used safely, ethically, and transparently, while fostering innovation. The Act categorizes AI systems based on their risk level and sets requirements for their deployment, with a strong emphasis on **accountability**, **transparency**, and **human oversight**. Understanding its provisions is essential for companies to ensure compliance and unlock AI's full potential responsibly.

Legislation

- The EU AI Act is a piece of legislation by the EU – it is legally binding.
- It regulates the development and use of AI systems.

Horizontal

- The EU AI Act is horizontal, meaning it is not industry-specific.
- It covers all industries and use cases.

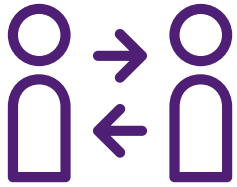
Risk-based

- The EU AI Act adopts a risk-based approach and classifies AI systems based on the risks they pose.
- The higher the risk, the more stringent the requirements and obligations are.

Extraterritorial

- The EU AI Act is extraterritorial.
- It does not only regulate EU companies, but also AI systems developed outside of EU that are placed on the EU market, or if the system outputs are being used within the EU.

Provider vs Deployer



- AI systems are developed and distributed through complex value chains.
- The Act differentiates between providers (i.e. developers) and deployers (i.e. users).

Staggered Implementation

- The EU AI Act has come into force in Aug 2024.
- There is a staggered implementation, starting at the 6-month mark.

EU AI Act

Shaping the Future of AI Regulation

	Examples	Requirements	
		Providers	Deployers
Prohibited AI Systems	• Predictive Policing • Social Scoring • Untargeted scraping of facial images • Emotion recognition in workplace	**Completely banned in EU**	
High-risk AI Systems	• **AI enabled Medical Devices** • Biometric identification (except for self-identification) • Human resources management (e.g. CV screening, systems used for promotion / termination decisions) • Credit scoring • Insurance pricing and risk assessment • Law enforcement, migration and border control • Critical infrastructure • AI systems used as safety component of products governed by EU law	• **Risk management** • **Data governance** • Technical doc • Record-keeping • Instructions of use • Human oversight • Accuracy, robustness and cybersecurity • Conformity assessment • Monitoring & incident reporting • **EU database registration**	• **Use AI system according to instructions** • **Human oversight** • **Fundamental rights impact assessment** • Monitoring & incident reporting
Limited Risk AI Systems	• AI chatbots and AI-powered search engines • AI-based recommendation systems (e.g. movie or shopping recommendations) • AI-generated content (e.g. AI-written news)	• Transparency obligations • Prevent manipulation or deception • Ensure data protection and security	• Ensure AI-generated content is labelled • Provide human oversight where needed
Minimal Risk AI Systems	• AI-driven spelling and grammar checkers • AI-powered spam filters and email categorization • Automated data entry tools	**No mandatory legal obligations**	

QMS Obligations in EU AI Act

Providers of high-risk AI systems are required to put in place a Quality Management System (QMS), which includes a number of aspects that are mapped to a Responsible AI (RAI) capability framework

RAI Capability Framework	QMS obligations in EU AI Act							
RAI RISK ASSESMENT	**Risk identification** Identifies the known and foreseeable risks of a high-risk AI system.	**Risk evaluation** Estimates the impact of risks under intended use or potential misuse.	**Risk mitigation** Minimizes AI system risks and mitigates residual risks within the organization's risk appetite.	**Testing of AI systems** Tests AI systems before launch to ensure risks align with the organization's risk appetite.				
OVERSIGHT & CONTROL	**Regulatory & compliance strategy** Defines the enterprise's strategy for compliance with the EU AI Act and other regulations, outlining key principles, procedures, and conformity assessments.	**Communication with authorities** Establishes communication channels and formats with authorities, customers, and stakeholders.	**Accountability framework** Defines roles and responsibilities for AI system development and management throughout its lifecycle.					
RAI EXECUTION EXCELLENCE	**Implementation guidebook** Documents comprehensive techniques, procedures, and actions for each stage of the AI system lifecycle.	**Post-market monitoring** Establishes a process for collecting, documenting, and analyzing performance data to ensure continuous compliance with the EU AI Act.	**Incident reporting processes** Defines the process for serious reporting, escalation procedures, and specified timescales.	**Technical requirements** Defines standards and methods to ensure AI system compliance with the EU AI Act.	**Resource management & training** Describes resource availability, skill qualification, and ongoing development of skilled workers.	**Data management: systems & procedures** Outlines systems and procedures for managing training, testing, validation, and runtime data, including pre-market.	**Record keeping** Defines what records need to be kept and for what amount of period	

RAI = Responsible AI

Impact on Life Science Companies

From Guidelines to Practice

The **EU AI Act** establishes **clear regulations** for AI systems in **life sciences**, ensuring **safety, accountability, and ethical AI deployment**. Companies must transition from **compliance guidelines** to **practical implementation** by addressing key challenges in AI governance, risk management, and regulatory adherence.

Challenge	Impact on Life Science Companies	Solution
AI Risk Classification	Companies must **assess AI systems** based on potential **risks to patient safety**, clinical outcomes, and regulatory compliance.	**Establish** clear **AI risk categorization frameworks** early in the process to ensure compliance with EU regulations and prioritize resources for high-risk AI systems.
Transparency & Explainability	**AI models** must be **interpretable**, especially in drug discovery, **clinical trials and clinical decision support systems**. Black-box models face regulatory hurdles.	**Integrate explainable AI (XAI) methodologies** to ensure clarity in AI decision-making, making it easier for stakeholders to trust and regulatory bodies to approve.
Data Integrity & Bias Mitigation	AI systems must **ensure fairness and prevent biases** in clinical data. Biased AI can lead to unsafe treatments and unreliable outcomes.	Develop **robust data governance frameworks** to monitor and eliminate biases in datasets, ensuring AI systems provide equitable and accurate results across all demographics.
Monitoring & Reporting	**Continuous evaluation of AI systems** in clinical trials, drug development, and routine use is necessary to maintain compliance and ensure patient safety.	**Implement real-time monitoring** systems that can flag issues and ensure regulatory bodies are informed of any deviations or risks in a timely manner.
Regulatory & Compliance	High-risk AI systems need **detailed documentation** to meet regulatory requirements.	Utilize automated **compliance tools to track and manage AI documentation**, helping companies stay compliant and streamline their regulatory submission processes.

Cyber Resilience Act (CRA)

The EU's Cyber Resilience Act is a regulation to strengthen cybersecurity requirements for products with digital elements (PDEs), including both hardware and software — AI systems included.

In-scope: Software or hardware product and its remote data processing solutions, known as "**products with digital elements**", that are logically or physically connected to a device or network

Out of scope:
- Medical devices, in vitro diagnostic medical devices (regulated by EU MDR / IVDR, motor vehicles, civil aviation, marine equipment *(all considered high-risk under EU AI Act)*
- National security or defence

=> Indirect impact on healthcare industry

	Default Category	Important Products (Annex III)		Critical Products (Annex IV)
		Class I	Class II	
Examples	All products with digital elements without a classification, e.g.: • Simple IoT devices • Photo-editing software	• Identity management • Password managers • Routers or modems • Personal wearable products	• Hypervisors • Firewalls • Intrusion detection • Tamper-resistant microprocessors	• Hardware devices with security boxes • Smart meter gateways • Smartcards
Manufacturer Obligations *(non-exhaustive)*	**Cybersecurity** (Annex I)**:** • Secure by default • Protect from unauthorised access • Protect data confidentiality and integrity, data minimisation • Reduce incident impact • Limit attack surfaces • Allow permanent setting removal **Vulnerability handling** (Annex I)**:** • Identify, document, address & remediate vulnerabilities • Disclose information about fixed vulnerabilities after security update • Regular tests and reviews **Other obligations** (Article 13)**:** • Instructions to user (Annex II) • Technical documentation (Annex VII) • CE marking, declaration of conformity • Include type, batch or serial no. • Designate single point of contact			
Conformity Assessment	Self-assessment	Self-assessment if harmonised standards are available and adopted Third-party conformity assessment if otherwise	Third-party conformity assessment	European cybersecurity certifications scheme

Confidentiality & Security

Privacy and confidentiality could be compromised by output data revealing sensitive patient data or proprietary research information. Breaches and adversarial attacks can lead to unauthorized access, damaging patient trust and exposing the organisation to legal and reputational risks.

CRA and EU AI Act Interlock

Article 12 of CRA defines the interlock with EU AI Act, in particular how compliance with the CRA cybersecurity requirements would provide presumption of conformity for the cybersecurity requirements in Article 15 of the EU AI Act.

	CRA	EU AI Act
Scope	Products with digital elements	AI systems
Classification of regulated products	Critical, Important (Class I & II) and default category	Prohibited, High-risk, AI systems with transparency obligations, GPAI models, GPAI models with systemic risks and default category
Value chain	**Manufacturer**, importer and distributor	**Provider, deployer**, importer and distributor
Cybersecurity requirements	Its entirety, details in Annex I	Article 15
Applicability of cybersecurity requirements	To all products with digital elements, regardless of classification	High-risk AI systems only
Applicability of conformity assessment requirements	To all products with digital elements; type of conformity assessment varies by classification	High-risk AI systems only

For products that are both classified as products with digital elements under CRA and as high-risk AI systems under EU AI Act:

Presumption of conformity	**Products that comply with CRA Annex I essential cybersecurity requirements and have a CRA EU declaration of conformity are deemed to comply with the cybersecurity requirements under Article 15 of EU AI Act**
Conformity assessment	• Products without a CRA classification: follow EU AI Act conformity assessment procedures • Critical or Important (Class I & II) products: follow CRA conformity assessment for cybersecurity requirements *(Art. 32 CRA)*, and also EU AI Act conformity assessment procedure *(Art. 43 EU AI Act)*
Other	• A single set of technical documentation shall be drawn up containing the information required by Annex VII of the CRA and by the EU AI Act *(Art. 31(3) CRA)* • Cybersecurity risk assessment under CRA can be part of EU AI Act risk assessment *(Art. 13(4) CRA)* • Manufacturers of the products may participate in the EU AI Act regulatory sandboxes *(Art. 12(4) CRA)* • Market surveillance authorities shall be the same under the EU AI Act and the CRA *(Art. 52(14) CRA)*

GPAI = General Purpose AI