Compliance & Risks

AI, Cyber, and the Medical Devices Mandate: The New High-Risk Regulatory Landscape

Author:
Fernanda Paro , Senior Regulatory Compliance Specialist, Compliance & Risks
Patricia Weathers , Regulatory Compliance Specialist, Compliance & Risks
Kahyeon Seo , Regulatory Compliance Analyst, Compliance & Risks

9th December 2025

Further regulatory developments may have occurred after publication. To keep up-to-date with the latest compliance news, sign up to our newsletter.

Table of Contents

AI, Cyber, and the Medical Devices Mandate: The New High-Risk Regulatory Landscape

01. About The Authors

Fernanda Paro, Senior Regulatory Compliance Specialist, Compliance & Risks

Fernanda is a Senior Regulatory Compliance Specialist with the Global Regulatory Compliance team, based in Barcelona. She monitors regulatory updates across North, Central, and South America, with deep expertise in Medical Device legislation.

As the project lead for a global initiative spanning multiple jurisdictions, Fernanda regularly delivers in-depth analysis on complex legal and compliance queries related to medical devices.

She holds an European Healthcare Compliance Certificate Program (EU HCCP), a postgraduate degree in Constitutional Law and a Master's in International Trade Law, specializing in MedTech compliance with a regulatory focus on Cybersecurity and Data Protection. A qualified lawyer in both Brazil and Portugal, Fernanda is fluent in Portuguese, English, and Spanish, currently learning French, and proficient in Italian.

01. About The Authors

Patricia Weathers, Regulatory Compliance Specialist, Compliance & Risks

Patricia joined Compliance & Risks as a Regulatory Compliance Specialist in 2024. She is a certified Lead Auditor for ISO 13485 and ISO 9001, and has spent over ten years working in Quality Compliance/Assurance in the medical device and automotive manufacturing sectors.

Additionally, her background includes research and information services at the academic level and in training development.

01. About The Authors

Kahyeon Seo, Regulatory Compliance Analyst, Compliance & Risks

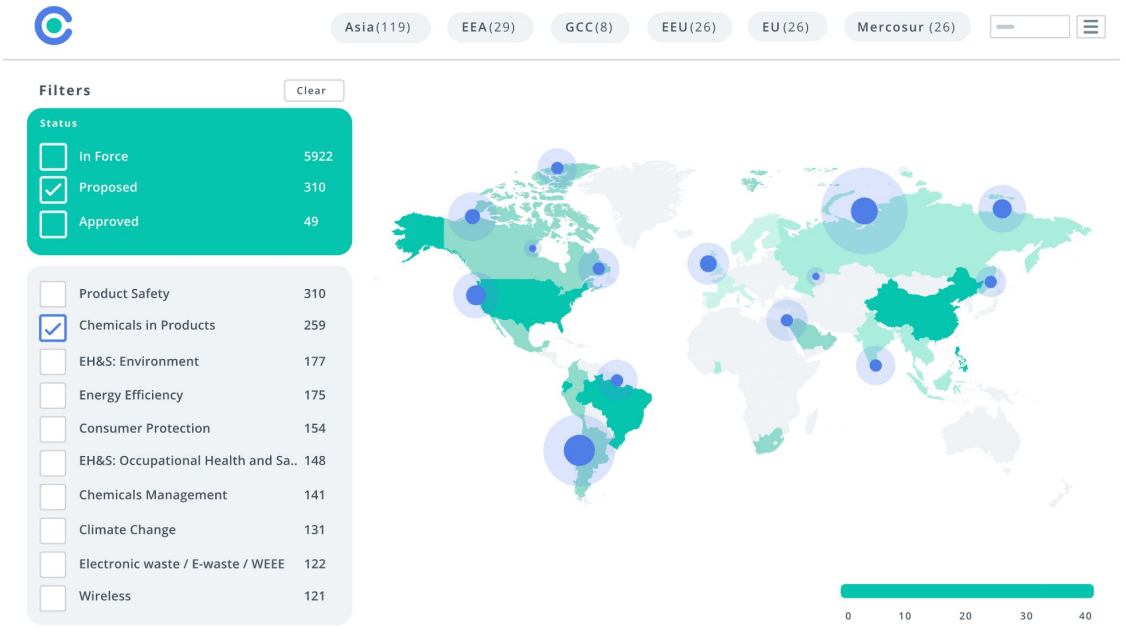
Kahyeon is a Regulatory Compliance Analyst at Compliance and Risks, having joined the company in 2024. She has academic backgrounds in Neuroscience and Criminology.

Prior to joining Compliance & Risks, Kahyeon worked in the raw material regulatory field, focusing on chemical compliance with regulations such as RoHS, REACH, TSCA, and toxicology standards, including MSDS.

She currently monitors regulatory updates in South Korea, Greece, and U.S. states, and serves as a secondary subject matter expert for medical devices.

Unlocking Market Access

Compliance & Risks empowers global enterprises to unlock market access and confidently navigate regulatory complexity. With a 20-year legacy in regulatory intelligence, we help beloved global brands manage product and corporate sustainability obligations, transforming compliance into a force multiplier for enterprise growth.



Our solution includes:

- **C2P:** The most advanced product compliance and corporate sustainability software on the market, helping you streamline your compliance process and unlock market access around the world.
- **Regulatory Content:** We provide the broadest and most comprehensive product compliance regulatory content on the market, monitoring 195+ countries, 20 industry sectors, 45 topics and 100,000+ regulatory sources.
- **Ask our Experts:** Direct access to our team of experts for support
- **C&R Sustainability:** Our new platform doesn't just track regulatory change; it generates intelligence next steps, tailored to your business. It's not just a dashboard. It's your ESG compliance brain: AI-native, human-verified, globally aware and ready with answers. Try a free trial **here**.

Why choose C2P?

- ✓ **Stay ahead** of regulatory changes with the world's most comprehensive regulatory database
- ✓ **Avoid delays** with alerts of changes to regulations & requirements in real time
- ✓ **Improve efficiency with powerful collaboration and workflow tools** to keep compliance evidence up-to-date & live linked back to Regulations, Standards & Requirements

Contact us to speak to one of our team today to learn how you can simplify your regulatory compliance process.

01. Introduction

The medical device industry is undergoing a profound digital transformation, driven by the ubiquitous integration of Artificial Intelligence (AI), software, and connectivity into all aspects of healthcare.

This transformation introduces powerful new capabilities - such as real-time patient data monitoring and predictive diagnostics - but also creates significant regulatory challenges. Consequently, compliance is no longer a simple technical requirement but a strategic enabler for MedTech innovation and global market access.

This comprehensive guide, based on our recent webinar "**Medical Devices in the Age of AI and Cybersecurity: Regulatory Insights**," serves as an essential roadmap for navigating this evolving landscape, focusing on the interwoven mandates of AI governance, cybersecurity, and data protection.

The core message is that compliance has moved from a reactive necessity to a proactive, strategic enabler for MedTech innovation, requiring a total product life cycle (TPLC) approach to AI governance and security.

The guide details the shifting frameworks in the European Union (EU), United States (US), and Asian markets, offering manufacturers an essential roadmap for navigating dual compliance, high-risk AI classification, and the legal codification of "security-by-design".

This guide was originally published on the 9th of December 2025. Further regulatory developments may have occurred after publication.

To keep up-to-date with the latest compliance news, **sign up to our newsletter.**

02. The Digital Transformation of MedTech

The healthcare and MedTech industries are undergoing a digital transformation driven by the deep integration of four core digital technologies: data, software, connectivity, and automation.

Data has become the most critical resource, leveraged through real-world evidence and device-generated information to enable continuous monitoring, predictive insights, and personalized patient care.

Software is now a core component of the medical product, giving rise to concepts like Software as a Medical Device (SaMD), AI algorithms, and digital therapeutics, which transform data into clinical and operational intelligence.

Connectivity, primarily through the Internet of Medical Things (IoMT), ensures that devices and systems exchange information securely and in real time, enabling remote diagnostics, connected care pathways, and interoperability.

Finally, automation helps reduce manual processes, improves traceability and data integrity, and supports compliance-by-design, making automated quality systems and risk controls essential for scaling innovative technologies without increasing the regulatory burden.

This integration of technologies not only modernizes healthcare but also makes compliance a strategic enabler, allowing MedTech companies to innovate faster and demonstrate safety and performance with greater agility.

Examples of this transformation include wearables for chronic-disease management, AI-based diagnostic tools, smart infusion pumps with remote alerting, and cloud-connected surgical robots.

03. Regulatory Convergence in Medical Devices

Regulatory convergence is the process where different countries or regions align their medical device regulations, standards, and practices, moving toward similar principles, comparable requirements, and a harmonized approach.

The goal is to make regulatory systems more compatible, predictable, and efficient globally. This convergence is needed for several reasons, including gaining faster access to safe medical devices by allowing companies to prepare documentation that works in multiple markets, reducing delays in bringing devices to patients.

It also reduces the burden for manufacturers by relying on shared terminology, common safety and performance standards, and comparable technical documentation formats, instead of redoing tests for each regulator.

Convergence improves patient safety and quality by encouraging the adoption of internationally recognized standards, such as ISO 13485 (Quality Management System), ISO 14971 (Risk Management), and IEC 60601 series (Electrical safety), as well as Good Regulatory Practices (GRPs) and reliance models.

Key elements driving this convergence include harmonized definitions and risk classification, standardized technical documentation (like the IMDRF Table of Contents), reliance and recognition mechanisms that accept FDA approvals or EU CE markings to avoid duplicate work, and post-market alignment, including vigilance reporting formats and adverse event terminology.

04. AI in Medical Devices: Distinctions and Risk Classification

A critical distinction in AI medical device regulation lies between Software as a Medical Device (SaMD) and Software in a Medical Device (SiMD).

SaMD is software with a medical purpose that functions independently of specific physical hardware, running on general platforms like the cloud, a phone, or a tablet, and is regulated as a standalone medical device.

An example is an AI algorithm analyzing MRI scans on a server. SiMD, conversely, is software integral to a physical medical device, such as embedded firmware or an operating system that controls the hardware, and is regulated as part of the overall hardware system.

This distinction is the primary step in determining the regulatory pathway.

Globally, a risk-based approach is being adopted.

European Union (EU):
Under the EU AI Act, virtually all AI-driven medical devices are automatically classified as High-Risk. This classification triggers the strictest compliance requirements, including a robust Quality Management System (QMS), extensive technical documentation, human oversight, and full transparency.

The EU approach requires a Dual Compliance Framework, where the AI medical device must comply with both the existing Medical Device Regulation (MDR) for safety and performance, and the new requirements of the AI Act for governance and transparency.

International Medical Device Regulators Forum (IMDRF):
The IMDRF classifies SaMD into four risk categories based on the significance of the information the AI provides (inform, drive, or diagnose) and the state of the patient's condition (non-serious, serious, or critical).

United States (US):
The FDA uses its existing device framework, classifying AI-driven devices as Class I, II, or III based on their potential for harm, with the intended use being the key determinant of the regulatory pathway.

For adaptive AI, the FDA is taking a Total Product Life Cycle (TPLC) approach, utilizing the Predetermined Change Control Plan (PCCP), a pre-approved plan outlining how the AI will learn and change without requiring a new submission for every modification.

05. Cybersecurity: The Mandate for Security-by-Design

The new legal reality for MedTech is cybersecurity-by-design.

This is a proactive approach that mandates integrating security measures from the earliest stages of development rather than treating them as a post-launch add-on. This global life cycle approach is the regulatory expectation for submissions in both the US and EU.

The full product life-cycle requires:

1. **Design:** Employing a Secure Product Development Framework (SPDF) and conducting AI threat modeling, using methods like STRIDE, to embed security based on standards like ISO 81001-5-1.
2. **Development:** Requiring secure coding practices and maintaining a Software Bill of Materials (SBOM).
3. **Verification:** Conducting comprehensive penetration testing and formally assessing the risk of Software of Unknown Provenance (SOUP) components.
4. **Deployment & Monitoring (Post-Market):** Continuous vulnerability and incident management is a core, legally mandated obligation.

Key legal pillars driving this are:

- **United States (US):** The FD&C Act (Section 524B) and the Patch Act legally mandate that manufacturers have a plan for vulnerability monitoring and post-market addressal, with the FDA Premarket Guidance detailing the submission rules and SBOM requirements. The TPLC approach is managed proactively via the PCCP.
- **European Union (EU):** This is a multi-layered system.
  - **MDR/IVDR (GSPR 1):** Establishes the high-level need for security and risk management.
  - **Cyber Resilience Act (CRA):** Mandates specific hard requirements, notably requiring the provision of an SBOM to users and guaranteeing a minimum of five years of post-market security support.
  - **NIS2 Directive:** Enforces the reporting rule, mandating an initial notification of a significant security incident to authorities within 24 hours.

06. Data Protection and Governance: The GDPR Foundation

Data protection ensures sensitive health data is handled lawfully, minimized, and accounted for, complementing cybersecurity which secures the underlying systems.

The European General Data Protection Regulation (GDPR) is the foundational cornerstone of digital health compliance, with its principles extending to all personal data processing, particularly health and genetic data classified as special categories.

The core GDPR principles are:

- **Lawfulness:** Processing personal data only when a valid legal basis exists.
- **Minimization:** Collecting only the minimum amount of data that is adequate, relevant, and necessary for the intended purpose.
- **Accountability:** Organizations must be able to demonstrate compliance, not just declare it. This involves maintaining Records of Processing Activities (RoPA), conducting Data Protection Impact Assessments (DPIAs) for high-risk processing (like AI diagnostics), and implementing technical and organizational security measures such as encryption, access controls, and audit logs.

For manufacturers, handling sensitive health data means integrating data protection by design and default into the entire product life cycle, including strong encryption and pseudonymization where possible, and aligning data retention limits with clinical needs.

Vendor Compliance is also a critical area, as manufacturers remain legally responsible for data processing even when outsourcing to vendors like cloud providers or data analytics tools. This requires mandating Data Processing Agreements (DPAs), conducting vendor security assessments, verifying sub-processors, and ensuring the vendor supports patient rights (access, deletion, rectification).

Finally, cross-border data transfer remains challenging, as personal data can only be transferred outside the EU/EEA under certain circumstances (e.g., adequacy decisions or appropriate safeguards aligned with Schrems II requirements). Manufacturers must prepare for the European Health Data Space (EHDS), which aims to introduce a unified framework for the primary and secondary use of electronic health data within the EU, requiring alignment with interoperability standards and consent management functions.

07. Global Compliance Strategies

In our recent successful webinar, "**Medical Devices in the Age of AI and Cybersecurity: Regulatory Insights**," our experts highlighted three key strategies for navigating the complexity of global MedTech regulation across Europe, South America, and the United States.

1. **Integrating AI Governance & Data Protection:**
   This strategy focuses on ensuring security, preventing bias, and mandating transparency across the device life cycle.
   a. **EU:**
      MDR (GSPR 17) requires security means against unauthorized data access at the design phase. The AI Act (Article 10) mandates data quality requirements to prevent algorithmic bias. GDPR requires "Privacy by Design and Default" for all patient data processing.
   b. **South America:**
      Brazil's RDC No. 751/2022 requires proof of efficacy for AI algorithms, and the LGPD (Law to Protect Personal Data) mandates informing individuals if their data is processed by AI (Article 20). Peru's AI Law emphasizes a risk-based approach with mandatory human oversight.
   c. **US:**
      The FDA's Cybersecurity Final document requires tangible deliverables like the SBOM in premarket submissions to mitigate supply chain risk. The PCCP sets the methodology for developing and validating data management practices and AI retraining.

2. **Cross-Functional Compliance Frameworks:**
   This strategy mandates the use of multidisciplinary teams and integrated Quality Management/Risk Management Systems to cover all aspects of the AI medical device.
   a. **EU:**
      MDR and the AI Act (Article 17) require dedicated QMS and risk management systems that use cross-functional teams (including data governance and human oversight) to plan, monitor, and evaluate the AI system's functions and safety.
   b. **South America:**
      Brazil (RDC 751) and Peru (Supreme Decree 115-2025) emphasize cross-functional compliance in their QMS documentation, requiring teams from data science, quality, and engineering to document AI risk and post-market compliance.
   c. **US:**
      The FDA's Total Product Life Cycle (TPLC) approach requires collaboration across design and post-market phases, with teams from data science, engineering, and clinical backgrounds focusing on bias mitigation and transparency.

3. **Continuous Monitoring & Proactive Compliance:**
The focus is on uninterrupted post-market surveillance to manage system drift, security vulnerabilities, and mandatory reporting.

   a. **EU:**
   MDR requires a systematic Post-Market Surveillance (PMS) plan and reporting of serious incidents (Vigilance). The AI Act (Article 61) mandates continuous post-market monitoring and log-keeping (Article 12) for traceability and corrective actions, focusing on accuracy, robustness, and cybersecurity.

   b. **South America:**
   Brazil (RDC 751) requires technovigilance for complaints and adverse events, including the detection and reporting of system drift. Peru (Decree 115) requires monitoring as a mandatory phase of the AI lifecycle to watch for drift and changes in patient data that could affect product bias.

   c. **US:**
   The final Cybersecurity guidance requires a proactive plan to monitor, detect, and address vulnerabilities, including timely updates. The overarching intent of the PCCP is proactive compliance, allowing for pre-authorized changes due to drift detection without needing a new premarket submission.

08. Future Trends and Regulatory Outlook

The regulatory outlook is characterized by the phased enforcement of the EU AI Act and a growing global focus on ethical governance.

- **AI Act Enforcement Timeline:** The AI Act formally entered into force in 2025. Obligations for high-risk AI systems, including those used in medical devices and healthcare applications, will become mandatory in 2026. Full enforcement, requiring compliance with conformity assessment, documentation, transparency, and post-market monitoring requirements, is expected by 2027.
- **Ethical AI and Transparency:** The focus is moving beyond technical safety toward ethical governance in healthcare. Key trends manufacturers must address are:
  - **Explainability and Human Oversight:** AI systems must be transparent, allowing users and regulators to understand their functioning and limitations.
  - **Bias Mitigation and Representativeness:** Developers must ensure data sets reflect real-world diversity to prevent discriminatory outcomes in diagnostics or treatment.
  - **Ethical Design and Accountability:** AI models must support human-centric decision-making.
  - **AI Labeling and Traceability:** High-risk AI systems must display clear conformity markings and documentation that demonstrates traceability throughout the life cycle.

- **Rising Cybersecurity Oversight and Audits:**
  Manufacturers should expect more audits and supervisory inspections by competent authorities and Notified Bodies. Mandatory incident reporting within strict timelines under NIS2 and increased scrutiny of supply chain security, particularly for AI models and cloud-based medical data services, will be the new norm.

- **The Future Role of Data Protection:**
  Data protection remains the heart of digital governance, expanding beyond the GDPR to include sector-specific instruments like the European Health Data Space (EHDS). Future compliance will rely on demonstrable ethical responsibility and continuous risk management. Proactively demonstrating stringent data protection and transparency will become a competitive advantage, winning the trust of hospitals, patients, and regulators.

09. Webinar Q&A

During the live webinar, numerous questions were sent in by our live audience. Our webinar presenters, **Fernanda Paro**, **Patricia Weathers**, and **Kahyeon Seo** provided expert answers to the most popular queries below.

Q1. How do you classify prescription glasses with software? Especially when the business model is to license the glasses and allow third parties to develop the software, where does the responsibility fall under? Is it with the company that manufactures or the one that develops the software?

It really depends on the designated purpose of the glasses with software and the market in which it would be provided. In these regions below, prescription glasses are categorized as medical devices, so the intended use of the software becomes key - basically, is its purpose to treat or monitor a patient's health condition? This can alter the usual practice that the entity responsible for placing the product on the market has regulatory compliance responsibility. Also consider which of the two is being licensed, the glasses or the software.

US: 21CFR, Part 3. Because both the prescription glasses (Class I device) and the medical software (SaMD) would be regulated devices, and could be categorized as a combination product, manufacturers and software developers would have to assess if the software is intended for medical purposes, such as monitoring a health condition like glaucoma or post-surgery monitoring. If the software is not part of treatment for a vision condition, then the manufacturer of the prescription glasses would most likely be responsible for medical device regulatory compliance in the US.

Europe: MDR (2017/745). Under the EU's MDR, Annex 8, Rule 11, medical device software is usually classified as Class IIa or higher, while prescription glasses are Class I. MDR's Article 22, software is usually classified separately from a device unless it is intended to drive the prescription glasses' function. The software developer would have to demonstrate its compatibility with the glasses, while the glasses' manufacturer would have to give the software developer information to confirm the glasses won't interfere with the software's operation or safety protocols.

China: NMPA (739). The NMPA holds that prescription glasses are considered a Class I device and the software as SaMD if it has a medical purpose, so smart glasses intended for a medical purpose could be considered Class II or III. The function of the software from simple monitoring (Class I) to AI diagnostics (Class III) will affect the level of the NMPA review to be done. The Software Develper of the therapeutic SaMD would most likely be responsible for the Class II/III registration, while the glasses manufacturer would be responsible for a Class I filing and ensuring the glasses meet standards to have the software.

Brazil: ANVISA RDC 751/2022. Under ANVISA, the Software Developer is deemed the responsible manufacturer because they must validate that the software (SaMD) will operate safely and effectvely with the prescription glasses.

Q2. Is the patch act separate from the section 524B?

The short answer is no. The Protecting and Transforming Cyber Health Care (PATCH) Act of 2022 is not separate from section 524B of the Federal Food, Drug, and Cosmetic Act (FDCA). Rather, the PATCH Act created section 524B by amending the FDCA through the 2023 Consolidated Appropriations Act.

In other words, the PATCH Act is the legislation Congress passed, and section 524B is the resulting statutory provision now embedded in the FDCA. As a result, these are not two distinct or parallel frameworks.

For regulatory and compliance purposes, section 524B is the operative legal requirement for manufacturers, while the PATCH Act represents the mechanism through which those requirements were introduced.

10. Conclusion

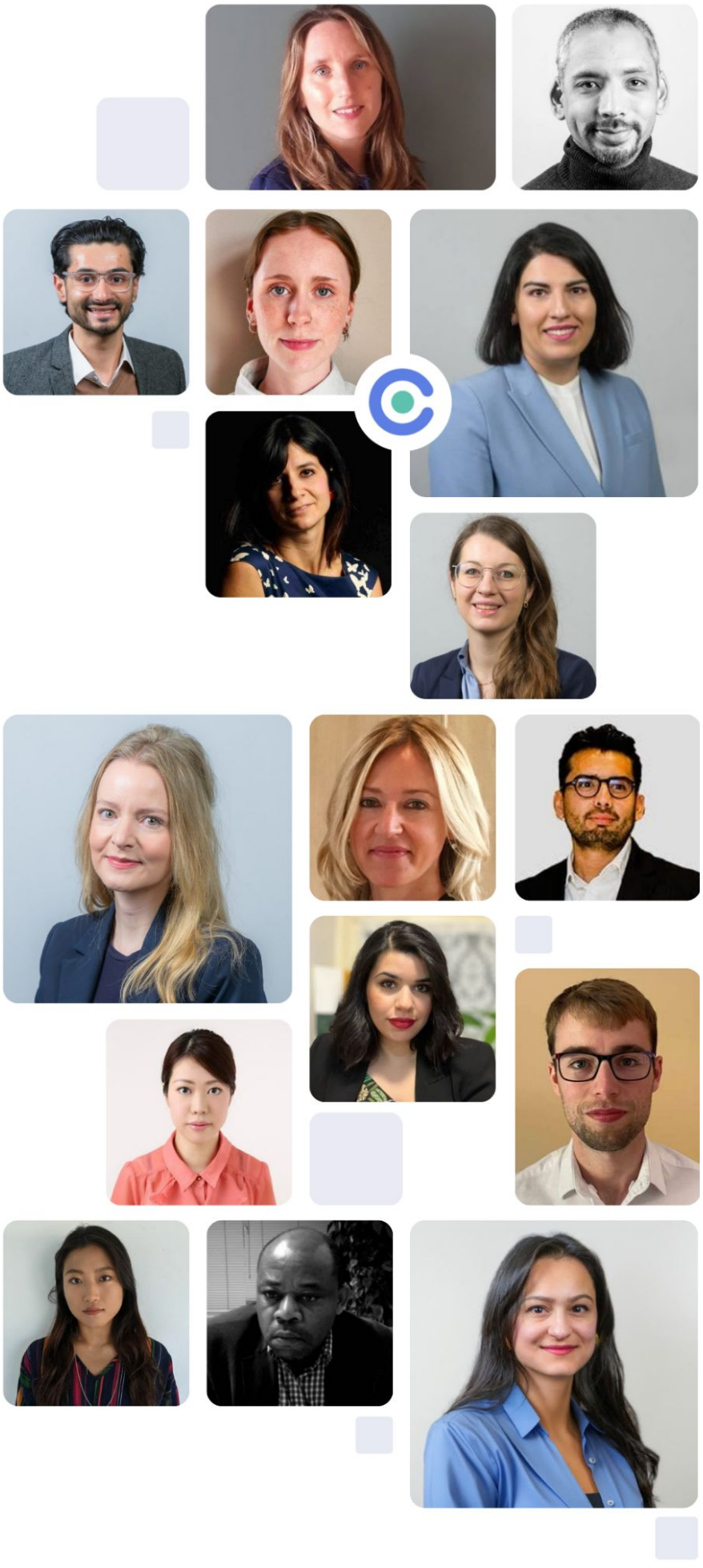
The regulatory environment for medical devices is undergoing a significant and structural change, demanding a shift toward a Total Product Life Cycle (TPLC) mindset.

The convergence of AI, cybersecurity, and data protection regulations means that compliance is no longer a checklist for market entry but a continuous, legally mandated obligation.

MedTech manufacturers must navigate the high-risk classification of most AI-driven devices under the EU AI Act , establish dual compliance systems (MDR/IVDR + AI Act) , and legally embrace cybersecurity-by-design (CRA and NIS2).

Organizations that move beyond technical conformity to embrace a proactive, integrated approach - demonstrating ethical responsibility, continuous risk management, and transparency - will be the best positioned to lead the next era of trustworthy healthcare innovation.

Compliance & Risks



Add 80+ Experts to Your Team

Stop Drowning in Regulatory Updates and Get Back to Business.

Feeling overwhelmed by the ever-changing world of global regulations? You're not alone. Keeping up with complex legislation like ESPR, RoHS, and China RoHS can feel like a full-time job, draining valuable resources from your core business.

What if you could add **80+ compliance experts** to your team?

With our Ask the Experts service, you can. Our global team of **50+ subject matter experts** and 30+ knowledge partners provides unparalleled expertise across a diverse range of products, geographies, and policy areas. We monitor regulatory changes daily and provide clear, concise answers to your most pressing compliance questions.

Gain instant access to:

- **In-depth knowledge:** Our experts possess deep understanding of complex regulations, including ESPR, RoHS, and China RoHS.
- **Rapid response:** Get quick answers to your questions, often within 30 minutes, freeing up your team to focus on other priorities.
- **Confidence and clarity:** Navigate regulatory complexities with assurance, knowing you have a team of experts backing you up.

Boost your compliance capabilities without expanding your headcount.

Empower your business today - begin your journey and **speak to a regulatory expert.**

Compliance & Risks

OUR NUMBERS

300+

CUSTOMERS WORLDWIDE

195

COUNTRIES COVERED

100,000+

REGULATIONS

→| complianceandrisks.com