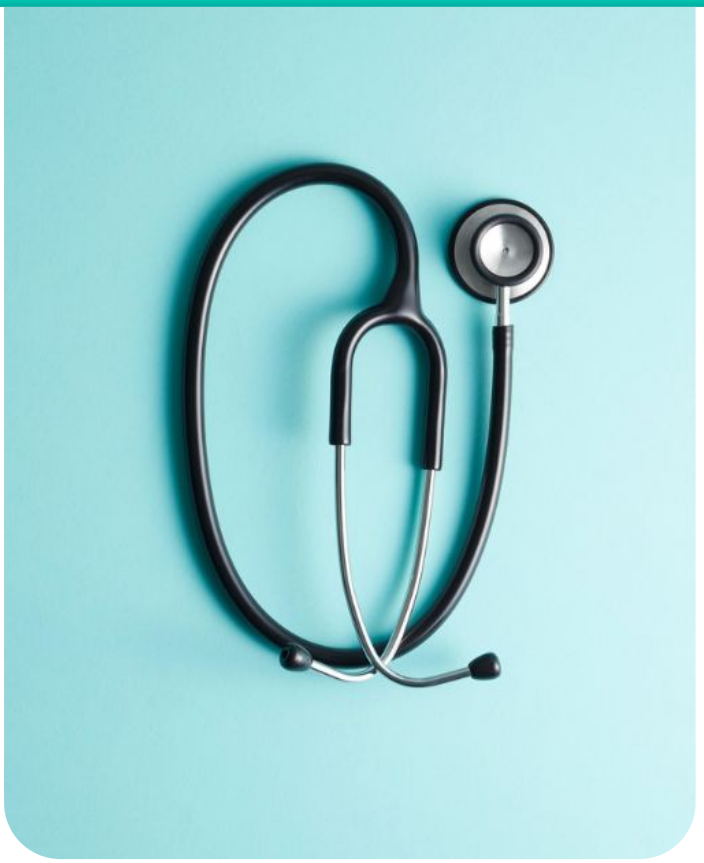
Compliance & Risks



Cybersecurity and AI Requirements in Medical Devices in Asia

Author:
Kahyeon Seo, Regulatory Product Compliance Analyst,
Compliance & Risks

20 August, 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

Cybersecurity and AI Requirements in Medical Devices in Asia

01. About The Author

Kahyeon Seo
Regulatory Product Compliance Analyst, Compliance & Risks

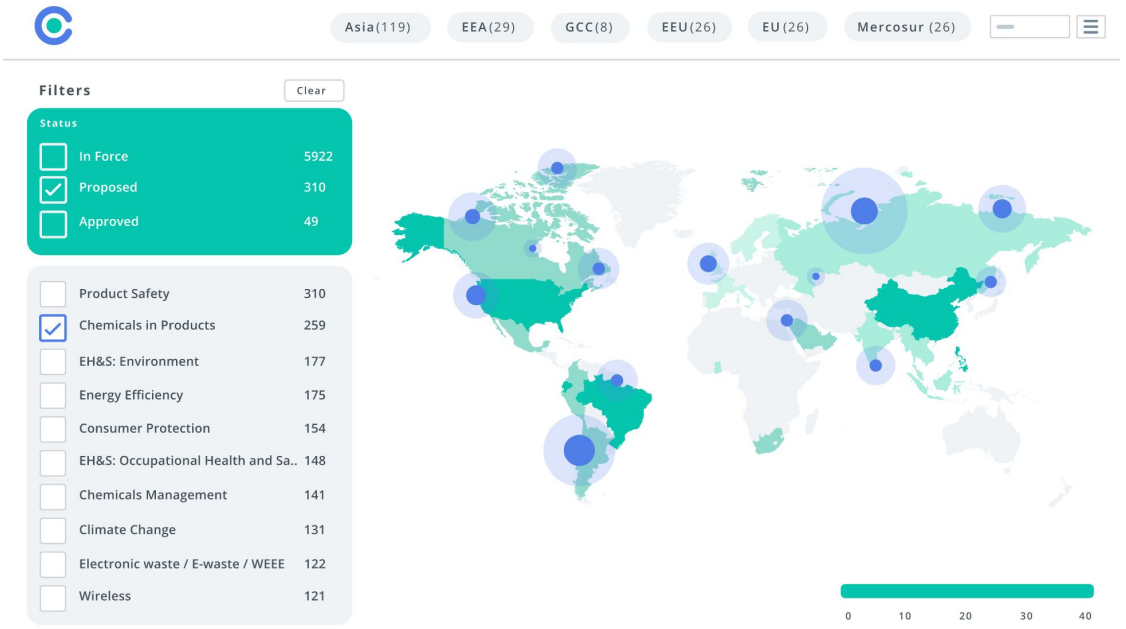
Kahyeon is a Regulatory Product Compliance Analyst in the Global Regulatory Compliance Team, specializing in medical devices, cosmetics, and South Korean regulatory frameworks.

With deep expertise in navigating complex compliance requirements, she provides critical insights to ensure product safety, market access, and adherence to evolving regulations. As a subject matter expert, Kahyeon supports global regulatory strategies and fosters alignment with international standards across healthcare and consumer product sectors.

Kahyeon holds a Bachelors in Neuroscience and Sociology of Law, Crime, and Deviance.

02. 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

Additionally, we offer:

- ✓ **Market Access Services:** Our Market Access team helps you understand your product compliance obligations by transforming regulations into actionable knowledge with tailored advice for you and your business.

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.

For more information, please visit http://www.complianceandrisks.com

03. Introduction

The increasing connectivity and software integration of medical devices have introduced new cybersecurity challenges that directly impact patient safety and data protection.

As cyber threats continue to evolve, regulatory authorities across Asia are implementing targeted frameworks to enhance medical device resilience against vulnerabilities.

This whitepaper reviews current and emerging cybersecurity regulations in South Korea, Japan, Taiwan, China, Hong Kong, and Singapore, and examines how artificial intelligence (AI) is shaping regulatory expectations.

It highlights how Asian jurisdictions are strengthening cybersecurity and AI oversight in medical devices through a combination of binding laws and evolving guidance. As AI becomes more deeply integrated into healthcare, new risks—such as data integrity breaches, model manipulation, and lack of transparency—are driving further regulatory refinement.

While national approaches vary, there is broad consensus that adaptive, lifecycle-based frameworks are essential to maintaining trust, safety, and resilience amid emerging digital threats.

04. Country-Specific Regulations

4.1. South Korea

In South Korea, cybersecurity and AI requirements for medical devices are regulated by the Ministry of Food and Drug Safety (MFDS). The country has developed a comprehensive framework covering the entire lifecycle of medical devices, particularly those with software and network capabilities. Regulatory oversight is anchored by the Digital Medical Products Act (Jan 2025), along with its Enforcement Decree and Enforcement Rule (Feb 2025), which provide a legal foundation for managing, certifying, and monitoring digital medical devices, including AI-enabled products.

The following Regulations and Guidelines are currently enforced in South Korea:

Guidelines on the Approval and Review of Medical Device Cybersecurity (Jan 2025)

- Applies to devices under Medical Devices Act, In Vitro Diagnostics Act, and Digital Medical Products Act.
- Covers Software in a Medical Device (SiMD) and Software as a Medical Device (SaMD).
- Core principles: Availability, Confidentiality, Integrity.
- Lifecycle risk management (analysis, control, post-market).
- Requires cybersecurity verification documents.

Regulation on Certification Criteria for Excellent Management Systems (Jun 2025)

- Manufacturers must prevent/respond to electronic intrusion (e.g., hacking, distributed denial-of-service (DDoS)).
- Requires physical, technical, and administrative controls.
- Appointment of security officers.
- Legacy device risk mitigation.
- Post-market vulnerability monitoring.

AI-Specific Controls (2025)

- **Standards for the Manufacturing and Quality Management of Digital Medical Devices (Apr 2025)**
- **Regulation on Certification Criteria for Excellent Management Systems (Jun 2025)**
    - Artificial Intelligence/Machine

Learning (AL/ML) digital medical devices require executive oversight in AI governance, including risk mitigation, role management, data quality and validation, model design, and continuous monitoring. Process integration controls, including documented records and traceability, are essential. Manufacturers must ensure training data quality and have a documented risk management plan for system and algorithm-specific risks.

Security Guidelines for Digital Medical Devices Against Electronic Intrusion (Apr 2025)

- Manufacturers must address defenses against data poisoning and evasion attacks, protection against tampering during data handling, model extraction/evasion prevention, and response plans for AI-related malfunctions. This covers quality management and cybersecurity for AI/ML-enabled devices, with focus areas including AI system governance, training data handling, model validation, continuous monitoring, and transparency of AI output.

South Korea leads with a binding, comprehensive framework under the Digital Medical Products Act and its 2025 guidelines. The system is mature, and while no major new legislation is pending, refinements are expected as implementation advances. This structured lifecycle approach ensures that both patient safety and data security are maintained throughout a device's market presence.

4.2. Japan

Japan's Pharmaceuticals and Medical Devices Agency (PMDA) has integrated cybersecurity requirements into its Quality Management System (QMS), supported by guidance from the Ministry of Health, Labor and Welfare (MHLW). Since the 2023 amendment adding cybersecurity rules for internet-connected devices, no new binding medical device regulations specific to cybersecurity or AI/ML have been introduced.

The **2025 Act on the Promotion of Research and Development and the Utilization of AI-Related Technologies (June 2025)** provides a broad framework to promote AI R&D but does not include specific rules for medical devices. Instead, medical device cybersecurity remains governed under sector-specific laws like the Pharmaceutical and Medical Device Act (PMD Act).

In the medical device sector, regulatory amendments and technical standards such as the **Amendment to the Standards for Medical Devices under Article 41(3) of the Pharmaceutical Affairs Act (April 2023)** require that, from April 2024, all newly approved and existing medical devices comply with cybersecurity provisions set out in Article 12, Clause 3 of the Essential Principles (EP) Criteria, based on the IMDRF Good Regulatory Practices (GHTF) EP document. This references the JIS T 81001-5-1 standard and mandates integration of security management into quality systems, addressing vulnerabilities, secure design and development, risk mitigation, configuration management with a Software Bill of Materials (SBOM), and vulnerability handling and disclosure.

The **JIS T81001-5-1:2023 standard (February 2023)**, aligned with IEC 81001-5-1:2021 on health software and health IT systems safety, sets cybersecurity requirements across the health software lifecycle. It covers product manuals, secure software development practices, vulnerability management, risk and configuration management, and problem resolution. The standard includes annexes providing guidance on threat modeling and alignment with IEC 62443-4-1 on establishing a secure development (SDL) for industrial automation and control systems (IACS) products.

Japan maintains a consistent regulatory landscape anchored by its 2023 cybersecurity amendment. While no new binding laws for medical devices are anticipated in the near future, the country continues advancing ongoing guidance and global harmonization efforts. Japan also leads international initiatives to establish common principles for AI management, currently favoring a flexible approach to AI governance. This flexible but thorough approach supports innovation while maintaining a steady commitment to safety.

4.3. Taiwan

Taiwan places strong emphasis on cybersecurity in medical device regulation. The Taiwan FDA (TFDA) mandates comprehensive measures throughout the device lifecycle, including protections against unauthorized access, regular risk assessments, security updates, and collaboration with healthcare IT professionals. Manufacturers must integrate cybersecurity controls from the design phase, following international standards such as ISO 14971 for risk management and IEC 62304 for software development.

The **Cybersecurity Guidelines for Medical Device Manufacturers (May 2021)** detail principles covering secure design, validation, documentation, and incident response. However, since 2021, Taiwan has not enacted standalone medical device regulations specifically addressing cybersecurity or AI/ML. These areas remain governed under general medical device laws and sector-specific guidance, with more targeted regulations and updated guidance expected soon to keep pace with evolving technologies.

Taiwan's Medical Devices Act (MDA) broadly defines medical devices to include instruments, materials, software, and related products intended for diagnosis, treatment, prevention, or structural modification of the human body. This definition explicitly covers AI, augmented reality (AR), virtual reality (VR) technologies, and medical personal protective equipment. AI/ML-based medical devices are currently regulated within this general framework without a separate pathway.

The TFDA recommends following internationally recognized standards like the U.S. FDA's Good Machine Learning Practice (GMLP) to ensure safety and quality. Additionally, the TFDA's **Guidance for Industry to Register Artificial Intelligence / Machine Learning - Based Software as Medical Device (AI/ML-Based SaMD) (Aug 2021)** requires detailed documentation of training methods, model architecture, and high-quality, well-segregated data to prevent bias.

While AI and cybersecurity are primarily regulated through existing laws and sector-specific guidance, ongoing updates are anticipated as part of Taiwan's broader digital health modernization efforts[1].

[1] *Refer to References No. 15*

4.4. China

Between 2022 and 2025, China significantly expanded its regulatory oversight of medical devices incorporating cybersecurity and artificial intelligence functions. Regulatory authorities such as the National Medical Products Administration (NMPA) have issued dedicated guiding principles addressing cybersecurity in both general medical devices and those with AI or mobile functionalities. These frameworks emphasize lifecycle risk management, secure data handling, system robustness, and alignment with China's broader cybersecurity policies.

The most recent advisory guiding principles are:

The **Guiding Principles for Registration and Review of Mobile Medical Devices (Revised May 2025)** include the following key requirements:

- Implementation of cybersecurity measures such as secure authentication, remote access control, and protection of locally stored data (e.g., encryption or deletion upon logout), which are critical for devices supporting clinical decision-making.
- Submission of comprehensive documentation, including terminal research reports, cybersecurity documentation, detailed product specifications for clinical and terminal functions, stability data, and clear instructions for use.
- Special consideration for devices intended for non-professional or home settings to ensure usability and safety.

There are also advisory guidelines from 2022 that outline robust cybersecurity and AI requirements:

The **Guiding Principles for Medical Device Cybersecurity Registration (March 2022)** require comprehensive, full-lifecycle cybersecurity for network-connected Class II and III medical devices, encompassing risk identification, protective design, threat detection, prevention, and recovery. Registration necessitates submitting detailed cybersecurity risk analyses, network security architectures, interface specifications, validation protocols, and patch management plans. AI-based diagnostic/monitoring software (typically Class III) must ensure secure data training, restricted AI output access, and AI decision traceability. Post-market obligations include continuous vulnerability monitoring, emergency patching, remote updates, coordinated disclosure, and ongoing risk reassessment.

China's **Guiding Principles for Registration and Review of AI Medical Devices (May 2022)** mandate cybersecurity for Class II and III AI medical devices, encompassing data security (confidentiality, integrity, availability, breach mitigation), secure development, and post-market monitoring (vulnerability, backup/recovery, compliance with healthcare IT and Chinese cybersecurity standards).

AI devices are categorized by function and risk. Performance evaluation covers accuracy, robustness, reproducibility, real-time operation, and explainability.

Manufacturers must use diverse, well-labeled datasets, conduct thorough testing, and maintain ongoing post-market monitoring.

Major algorithm changes require re-approval; adaptive self-learning is prohibited without separate validation.

China remains active in maintaining detailed cybersecurity and AI frameworks aligned with national data governance policies.

While no major new regulations are expected in 2025, ongoing technical updates and enforcement notices are likely. Current regulations focus on ensuring the safe and secure use of medical devices while protecting patient data privacy and security.

As cybersecurity rules in China continue to evolve, manufacturers must stay informed of changes and work closely with regulators to ensure compliance and device security.

4.5. Hong Kong (China)

As of 2025, Hong Kong has established a regulatory framework for medical devices incorporating cybersecurity and artificial intelligence (AI) through the Medical Device Administrative Control System (MDACS). The Department of Health (DH) has issued Technical References (TR-007 and TR-008) to guide the classification, listing, and cybersecurity requirements for Software as a Medical Device (SaMD) and AI-enabled medical devices. These references align with international standards, emphasizing design controls to address cybersecurity risks throughout the device lifecycle.

The **Technical Reference Software Medical Devices and Cybersecurity TR-007 (Dec 2023)** outlines requirements for Software in Medical Devices (SiMD) and Software as a Medical Device (SaMD), focusing on lifecycle cybersecurity. It provides guidance on classification, listing, and cybersecurity requirements under the Medical Device Administrative Control System (MDACS). The most recent revisions were made **May 2025**, including:

- **Scope & Classification** – Medical-purpose software is classified as a medical device under MDACS using TR-003/TR-006 risk-based principles. Software in hardware (SiMD) is classified with the device; standalone software (SaMD) is listed separately with Medical Device Division's (MDD) approval.
- **Technical Documentation** – Requires Quality Management System (QMS) (ISO 13485), Essential Principles compliance (TR-004), clear labeling, ISO 14971 risk management (incl. cybersecurity), and clinical evaluations showing EP conformity and risk-benefit analysis.
- **Software Requirements** – Must meet IEC 62304 verification/validation, maintain versioning and traceability, manage cybersecurity risks (development, technical, environmental, physical, social engineering), and submit change applications for updates.
- **Cybersecurity** – Integrate risk management across lifecycle, prohibit default passwords, ensure vulnerability monitoring/disclosure, align with ISO 27032, ISO/IEC 27001, and local guidelines (e.g., Hong Kong Digital Policy Office).

The 2025 revision of TR-007 strengthens the connection between TR-007 and TR-008, ensuring consistency in regulatory expectations for AI-enabled medical devices.

Artificial Intelligence Medical Devices (AI-MD) TR-008 (Jan 2024) provides additional requirements specific to AI-enabled medical devices regulated under MDACS to ensure regulatory alignment with TR-007. The most recent revisions were made November 2024, including:

- **Scope and Application**
  - Applies to all AI-MD regulated under the Medical Device Administrative Control System (MDACS).
- **Classification and Listing Requirements**
  - AI-MD classification follows risk-based principles per TR-003 (general devices) and TR-006 (IVD devices).
  - Detailed records must be maintained for Medical Device Division (MDD) review, including dataset details (input data, preprocessing, source, labeling, and handling of training, validation, and testing data), AI/ML model descriptions with performance validation and

clinical relevance, and documented deployment workflows covering output use, update schedules for continuous learning, change reporting, and version control with traceability.

- **Post-Market Monitoring**
  - Manufacturers must establish active post-deployment monitoring with local partners to detect and prevent model drift or accuracy loss, report findings, submit change applications or corrective actions to the MDD, and maintain post-market performance data for submission upon request.

Hong Kong's voluntary MDACS system incorporates robust technical references on cybersecurity and AI, but no move toward mandatory regulation is currently expected. The emphasis remains on alignment with international standards and best practices.

For submissions involving software-based or AI-enabled medical devices, ensure consistency between TR-007 and TR-008, and review updated terminology and references to remain aligned with the latest regulatory requirements.

Please note that medical device manufacturers in Hong Kong are not required to comply with mainland China's medical device regulations unless they plan to market or register their products there.

4.6. Singapore

Medical device cybersecurity is overseen by the Health Sciences Authority (HSA), in collaboration with the Cyber Security Agency of Singapore (CSA) and the Ministry of Health (MOH). The framework aligns with the Health Products Act, ASEAN Medical Device Directive (AMDD), and International Medical Device Regulators Forum (IMDRF).

Singapore has developed a tiered Cybersecurity Labeling Scheme and best practice guidelines, with the draft Guide on Best Practices for Medical Device Cybersecurity having completed public consultation. These frameworks are expected to be formalized soon, positioning Singapore as a regional benchmark-setter. They embody a forward-looking approach that balances innovation with patient safety, ensuring emerging cybersecurity threats and AI-specific risks are effectively managed within a robust and evolving regulatory framework.

The latest updates in Singapore involve:

The Cybersecurity Labeling Scheme for Medical Devices [CLS(MD)] (Oct 2024)

- Introduces a tiered labeling system promoting transparency and best practices across device lifecycles, ranging from baseline to advanced evaluations (Levels 1–4).
- It sets rules on label validity, renewal, documentation, and criteria for suspension.

The Draft Guide on Best Practices for Medical Device Cybersecurity (Mar 2025)

- Outlines safeguards for secure design, risk mitigation, security testing, incident response, and post-market monitoring.
- Devices must include strong authentication, secure configurations, threat modeling, and layered incident response strategies with documented patch management.
- Real-time monitoring and vulnerability logging support early threat detection.
- A Software Bill of Materials (SBOM) is required for traceability of third-party components to manage vulnerabilities efficiently.

For AI-powered devices, additional security focuses include:

- Ensuring data integrity, model robustness, explainability, audit trails, and securing third-party algorithms and datasets.

05. Conclusion: Evolving Cybersecurity and AI Oversight in Asia

Across Asia, the regulatory landscape for medical device cybersecurity is becoming more sophisticated, with varying degrees of prescriptiveness and enforcement.

South Korea, Singapore, and China have adopted detailed, binding frameworks that embed security into the entire product lifecycle, while Japan and Taiwan align closely with international standards to facilitate global market access. Hong Kong, though less formalized, still encourages adherence to recognized best practices.

A common trend is the heightened attention to AI-enabled devices, reflecting the dual challenge of managing cybersecurity risks and ensuring algorithmic transparency. Another shared priority is post-market monitoring, which ensures devices remain secure against evolving threats.

For manufacturers, this means that cybersecurity compliance in Asia increasingly requires early integration into product design, rigorous documentation, and proactive vulnerability management. For regulators, ongoing collaboration with industry will be critical to balance innovation with patient safety. As these frameworks mature, Asia is poised to play a central role in shaping global norms for medical device cybersecurity—especially in the era of AI-driven healthcare.

Want to find out how you can stay on top of the changing Medical Devices compliance landscape? Start a conversation with us today!

06. References

1. South Korea: Digital Medical Products Act Enforcement Rules, Ordinance No. 2025, 2025
2. South Korea: Digital Medical Products Act Enforcement Rules, Ordinance No. 2025, 2025
3. South Korea: Approval and Review of Medical Device Cybersecurity, Guidelines Document, January 2025
4. South Korea: Certification Criteria for Excellent Management Systems, Regulation, MFDS Notice No. 2025-38
5. South Korea: Standards for the Manufacturing and Quality Management of Digital Medical Devices
6. South Korea: Certification Criteria for Excellent Management Systems, Regulation, MFDS Notice No. 2025-38
7. Japan's 2025 Act on the Promotion of Research and Development and the Utilization of AI-Related Technologies
8. Japan: Standards for Medical Devices under Article 41 (3) of Pharmaceutical Affairs Act, Notice No. 122, 2005 - Amendment - (on cybersecurity of medical devices) Notice No. 67, 2023
9. Essential Principles in Japan based on GHTF/SG1
10. Japan: JIS T81001-5-1:2023 Health Software and Health IT Systems Safety, Effectiveness and Security Part 5-1: Security-Activities in the Product Life Cycle, Standard, February 2023
11. Lexology: Summary Overview of the Japan AI Bill
12. Taiwan: Medical Device Cybersecurity Guidelines for Manufacturers, Announcement No. 1101603391, 2021
13. Taiwan: Medical Device Cybersecurity Guidelines for Manufacturers, Announcement No. 1101603391, 2021 (English Version)
14. US FDA: Good Machine Learning Practice for Medical Device Development: Guiding Principles
15. Taiwan: Guidance for Industry to Register Artificial Intelligence / Machine Learning - Based Software as Medical Device (AI/ML-Based SaMD)
16. Taiwan Ministry of Health and Welfare Launches Data System to Aid Medical AI
17. China: Guiding Principles for Registration and Review of Mobile Medical Devices (2025 Revised Edition)
18. China: Guiding Principles for the Registration Review of Medical Device Cybersecurity, Announcement No. 7, 2022
19. China: Registration and Review of Artificial Intelligence Medical Devices, Guiding Principles, Announcement No. 8, 2022
20. Hong Kong: Software Medical Devices and Cybersecurity Technical Reference: TR-007 (May 2025)
21. Hong Kong (China): Artificial Intelligence Medical Devices (AI-MD), Guidance Document, TR-008, January 2024
22. NordPacificMedical Article on Hong Kong: Revision of Technical Reference "Software Medical Devices and Cybersecurity" (TR-007)
23. Singapore: Cybersecurity Labelling Scheme for Medical Device Publications
24. Singapore: Best Practices for Medical Device Cybersecurity, Draft Guidance - Public Consultation, March 2025
25. Cybersecurity Regulations for Medical Devices in Asia

Compliance & Risks

OUR NUMBERS

300+

CUSTOMERS WORLDWIDE

195

COUNTRIES COVERED

100,000+

REGULATIONS

→| complianceandrisks.com