LAN
Lifesciences Asia-Pacific Network

Medical Device Cybersecurity

2023

Table of Contents

Overview

As medical devices become more interconnected and data-driven, cybersecurity and personal data privacy have become critical issues for medical device manufacturers expanding across the diverse Asia-Pacific regulatory landscape. Digital health technologies and internet-connected devices are creating new governance challenges that Asia-Pacific jurisdictions are only beginning to address through legal frameworks aimed at mitigating threats and ensuring proper data protection in healthcare.

For medical device companies targeting growth across Asia-Pacific, understanding this complex and rapidly evolving regulatory environment is essential to ensuring compliance and security. This guide has been designed to examine the key cybersecurity and data privacy regulations that medical device software must navigate in nine major Asia-Pacific markets, including Australia, China, India, Indonesia, Japan, South Korea, Singapore, Thailand, and Vietnam. We provide a high-level summary of the cyber and privacy regimes medical device companies must grapple with as they expand in the Asia-Pacific region and integrate software and connectivity into their medical products.

Australia

Latest update: August 2023

Definition and scope		
1.	In your jurisdiction, what is the legal definition for medical devices?	In Australia, 'medical device' is defined in section 41BD of the Therapeutic Goods Act 1989 (Cth) (**TG Act**) as: – any instrument, apparatus, appliance, software, implant, reagent, material or other article (whether used alone or in combination, and including the software necessary for its proper application) intended to be used for human beings for the purpose of one or more of the following: - diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease; - diagnosis, monitoring, treatment, alleviation of or compensation for an injury or disability; - investigation, replacement or modification of the anatomy or of a physiological or pathological process or state; - control or support of conception; and/or - *in vitro* examination of a specimen derived from the human body for a specific medical purpose;* and that does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but that may be assisted in its function by such means; or – any instrument, apparatus, appliance, software, implant, reagent, material or other article specified under subsection (2A) of the TG Act (i.e. a notice published in the Government Gazette or on the Australian Department of Health website); or – any instrument, apparatus, appliance, software, implant, reagent, material or other article that is included in a class of instruments, apparatus, appliances, software, implants, reagents, materials or other articles specified under

	subsection (2B) of the TG Act (i.e. the Secretary of Health by legislative instrument); or – an accessory to an instrument, apparatus, appliance, software, implant, reagent, material or other article covered by the above points; or – a system or procedure pack. *Note that the purpose of a device is ascertained from the information supplied on or in the following sources: – the labelling on the main equipment; – the instructions for using the main equipment; – any advertising material relating to the main equipment; and/or – technical documentation describing the mechanism of action of the main equipment.
2. (a) In your jurisdiction, are all types of health care related software (i.e., computer programs, applications, or systems specifically designed to support and enhance various aspects of healthcare delivery and management, including those in independent form and those attached to a physical medical device) can regarded as medical device based on the above definition? (b) If not all the health care related software can be covered by the definition of medical devices, is it clearly defined which kinds of medical related software will be regulated as a medical device and which are not?	In Australia, the general position is that any software, which meets the definition of a medical device will be regulated and require entry into the Australian Register of Therapeutic Goods (**ARTG**) before it may be supplied, unless it is excluded or is a clinical decision support software that is exempt. **<u>Excluded medical software</u>** There are some defined forms of software that are excluded as medical devices. These are listed in a schedule to the Therapeutic Goods (Excluded Goods) Determination 2018 (Cth). Examples of excluded medical devices include: – Software that is: (a) intended by its manufacturer to be used by a consumer for the self-management of an existing disease, condition, ailment or defect that is not a serious disease or serious condition, ailment or defect; and (b) not intended by its manufacturer to be used: (i) in clinical practice; or (ii) in relation to a serious disease or serious condition, ailment or defect; or (iii) for the purpose of diagnosis, treatment, or making a specific recommendation or decision about the treatment of a disease,

	condition, ailment or defect that is not a serious disease or serious condition, ailment or defect. – Software or a combination of software and non-invasive hardware that is: (a) intended by its manufacturer to be used by a consumer to promote or facilitate general health or wellness by measuring or monitoring (through non-invasive means) a physical parameter, such as movement, sleep, heart rate, heart rhythm, temperature, blood pressure or oxygen saturation; and (b) not intended by its manufacturer to be used: (i) in clinical practice; or (ii) for the purpose of diagnosis, screening, prevention, monitoring, prediction, prognosis, alleviation, treatment, or making a recommendation or decision about the treatment, of a serious disease or a serious condition, ailment or defect. This is not an exhaustive list. **Exempt clinical decision support software** Medical software that is a clinical decision support system software, which facilitates, supports and enables clinical practice (e.g. web-based applications that provide information about particular diseases, software intended to analyse x-rays or software that collects and records data from a glucose monitoring device) is exempt under the Therapeutic Goods (Medical Devices) Regulations 2002 (Cth) (**Regulations**) if it meets the following criteria: – it is not intended to directly process or analyse a medical image or a signal from another medical device; – it is intended by its manufacturer only for providing or supporting a recommendation to a health professional about preventing, diagnosing, curing or alleviating a disease, ailment, defect or injury in persons; and – it is not intended by its manufacturer to replace the clinical judgement of a health care professional to make a clinical

	diagnosis or treatment decision regarding an individual patient.
General regulatory requirements	
3. For medical software that is regulated as a medical device ("**Medical Device Software**"), what regulatory steps (e.g., additional clinical trials, approvals, tests, maintenance, supplementary registration after software update) are required to be completed before it can be approved for market launch and during the post-marketing period?	Software classified as a medical device cannot be lawfully supplied in Australia unless it is included on the ARTG. A sponsor must apply to the Therapeutic Goods Administration (**TGA**) to include their device on the ARTG. The TGA applies a risk-based approach to assessing whether the medical device complies with the following two requirements to be listed on the ARTG: 1. **Essential principles** – The 'essential principles' are a list of requirements set out in Schedule 1 of the Regulations. These requirements are not prescriptive, but rather are high level principles, the application of which vary depending on the type and characteristics of the device. It is a matter for the manufacturer to determine which essential principles apply to their device. The essential principles generally fit into two broad categories: 1) general principles on the safety and suitability of the medical device; and 2) principles about design and construction which includes: – the chemical, physical and biological properties; – control and minimisation of infection and microbial contamination; – removal or minimisation of risks associated with use (e.g. injury, ageing of materials, loss of accuracy and disposal of waste substances); – minimisation of exposure to radiation; – protection against risks associated with energy sources (if relevant); and – information to be provided with the medical device.

	2. **Conformity assessment evidence** – Evidence that a device has undergone an appropriate conformity assessment procedure must be held before a device can be included in the ARTG. These requirements vary depending on the classification of the medical device. Under the Regulations, medical devices are classified based on their intended purpose, degree of invasiveness, duration and location of use and source of energy. For example, Class I are 'low' risk medical devices that include surgical retractors and tongue depressors, and Class III are 'high' risk medical devices that include heart valves and major joint replacement implants.
Cybersecurity requirements	
4. Is Medical Device Software subject to general cybersecurity regulations in your jurisdiction? If so, (a) how do these regulations apply to Medical Device Software? (b) Can you provide a brief introduction of the general cybersecurity requirements that are applicable to the Medical Device Software?	(a) Medical device software may be subject to the following general cyber security regulations in Australia. 1. Security of Critical Infrastructure Act 2018 (Cth) (**SOCI Act**) – the SOCI Act promotes the resilience and protection of Australian 'critical infrastructure assets'. The SOCI Act applies to owners or operators of certain infrastructure in the health care and medical, energy, communications, data storage or processing, financial services and markets, water and sewerage, higher education and research, food and grocery, transport, space technology, and defence industries. Currently, medical devices do not fall within the direct ambit of the SOCI Act. However, at the time of writing, 'critical hospitals' that have a general intensive care unit are captured by the SOCI Act with respect to the healthcare and medical industry. The SOCI Act sets out a range of obligations, but with respect to cybersecurity specifically, owners of operators of certain critical hospitals must develop and comply with a critical infrastructure risk management programme (**CIRMP**). A CIRMP is a written programme, which requires a responsible entity for a critical infrastructure asset:

	• to identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset; • so far as it is reasonably practicable to do so—to minimise or eliminate any material risk of such a hazard occurring; and • so far as it is reasonably practicable to do so—to mitigate the relevant impact of such a hazard on the asset. Depending on the type of medical device software, the above could apply such that the medical software will be subject to a CIRMP. 2. Privacy Act 1988 (Cth) (**Privacy Act**) – the Privacy Act is the general law in Australia in relation to the privacy of personal information and includes, in Schedule 1, the Australian Privacy Principles (**APPs**) which govern the collection and handling of personal information by regulated entities. In particular, APP 11 requires an APP entity to take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure. While APP 11 does not apply specifically to medical software, it will be relevant in the context of cloud-based medical software-as-a-service, which stores patient information. In this scenario, the provider of that software service (and any contracted data centre operators) would need to comply with APP 11 to the extent that they hold personal information. See question 6 for further information on the Privacy Act.
5. In addition to the generally applied cybersecurity requirements, are there any cybersecurity requirements that are specifically set for Medical Device Software, including any cybersecurity related requirements in its development, testing, deployment, and maintenance of Medical Device Software?	The specific cyber security requirements that apply to medical devices form part of the list of 'essential principles' set out above in section 3, which must be complied with in order to have the device included on the ARTG. These principles recognise that cyber security is not limited to protecting the privacy of patients but also safeguard the health and safety of those patients by minimising breaches that may have the potential of denying intended therapy or altering the function of the device.

	The TGA's guidance for industry on medical devices and cyber security emphasise the following essential principles: – to ensure that risks are 'acceptable' when weighed against the intended benefit to patients and are compatible with a high level of protection to health and safety; – to minimise risks associated with the use of the device by identifying hazards, adopting a policy of safe design and construction, adopting adequate protection measures for uneliminated risks and inform users of residual risk; – to ensure that programmable medical devices are designed according to the 'best practice' in relation to software, security and engineering and includes (among others and where appropriate): - protection against unauthorised access, influence or manipulation; - minimisation of risks with known cyber security vulnerabilities; and - disclosure of known vulnerabilities. To comply with the risk minimisation principles, the TGA has provided guidance to manufacturers of medical devices on completing pre- and post-market risk management activities. The guidance provides the following: 1. **Pre-market risk management**: Manufacturers are required to address cyber security risks during the design and development process. This includes: • general considerations, such as the development approach; administration protocols; application of standards; risk management strategies; infrastructure, manufacturing and supply chain management; and provision of information for users; • technical considerations, such as cyber security penetration testing; modularised design architecture; operating platform security; emerging software; and trusted access and content provision; • environmental considerations for the device's intended use, such as connecting to networks and uploading or downloading data;

	• physical considerations, such as mechanical locks on devices and interfaces, physically securing networks, waste management (preventing capture of sensitive paper-based information); and • social considerations, such as designing out or minimising social-engineering threats (e.g. phishing, impersonation, baiting, tailgating). 2. **Post-market risk management:** Manufacturers and sponsors are required to continually assess and take action on medical device cyber security risks such as: • developing a compliant risk management strategy that demonstrates how medical device cyber security risk is reviewed and updated; and • considering cyber security events that do not appear to immediately impact a medical device (still part of the cyber security threat landscape) as part of a compliant medical device cyber security risk management strategy.
Data protection requirements	
6. How is data collected and processed by Medical Device Software regulated in your jurisdiction?	Australia's federal and state/territory level privacy laws regulate the collection and handling of health information. At the federal level, the Privacy Act sets out the general law with respect to the handling of personal information (including health information) by Australian Government agencies and private sector organisations (subject to certain exceptions). In addition, the MyHealth Records Act 2012 (Cth) (**MyHealth Records Act**) prescribes when and how 'My Health Record' information may be collected, used and disclosed. Unauthorised collection, use or disclosure of a 'My Health Record' will amount to a breach of the MyHealth Records Act and an interference with privacy. At the state and territory level, there are equivalent laws, which apply to the handling of health information by the relevant state or territory government agencies and may (in some cases) apply to the private sector. These include: (a) in New South Wales, the Health Records and Information Privacy Act 2002 (NSW), which governs

		New South Wales public sector agencies and private sector health service providers; (b) in Victoria, the Health Records Act 2001 (Vic) which governs Victoria public sector agencies and private sector health service providers; (c) in the Australian Capital Territory, the Health Records (Privacy and Access Act 1997 (ACT), which governs Australian Capital Territory public sector agencies and private sector health service providers; (d) in Queensland, the Information Privacy Act (2009) (Qld), which governs only Queensland public sector agencies; (e) in Western Australia, the Health Services Act 2016 (WA), which governs Western Australian public sector agencies and private sector health service providers; (f) in the Northern Territory, the Information Act 2002 (NT), which governs Northern Territory public sector agencies and private sector health service providers; and (g) in Tasmania, the Personal Information Protection Act 2004 (TAS), which provides individuals access to personal information that is held by the Department of Health (Tasmania).
7.	Is there any data localisation requirement for the data generated or processed via the Medical Device Software?	Yes. In some Australian jurisdictions (e.g. New South Wales and Victoria), health records laws restrict disclosure of health records outside of the relevant state or territory unless certain criteria are satisfied (e.g. the individual consents to the transfer; a substantially similar protective regime will apply to the disclosed records; the transfer is necessary for the performance of a contract between the individual and the organisation; or the organisation has taken reasonable steps to protect the information consistent with that jurisdiction's privacy principles).
8.	From a compliance perspective, are the above regulatory requirements being fully implemented in practice? Are there any compliance risks that the Medical Device Software operators may need to note?	There are numerous offences under the TG Act with respect to the supply of therapeutic goods (including medical software if not excluded or exempt). These are: – supplying therapeutic goods not included on the ARTG; – importing and/or supplying medical devices that do not meet the essential principles;

	– failing to apply conformity assessment procedures; – misrepresenting medical devices; and – failing to report adverse events. If a responsible entity commits an offence, the TGA will often assist that entity to achieve compliance by way of education and advice. However, the TGA has the power to exercise various compliance and enforcement tools, particularly if: (a) the entity has repeated breaches and is not willing to comply; and/or (b) the alleged breach is such that there is a likely impact on the consumer's ability to use therapeutic goods safely or appropriately. The TGA's compliance avenues include: (a) **warning letters**: warning letters may be issued for low compliance risks and may outline corrective action; (b) **suspensions**: the TGA may suspend a therapeutic good, which means the good may not be imported into, exported from, manufactured or supplied within Australia by the entity during the suspension period; (c) **cancellations**: in instances of deliberate non-compliance or the discovery of non-compliant systems, therapeutic goods may be cancelled by the ARTG; (d) **recall actions**: a recall action is a set of prescribed actions set out in the Uniform Recall Procedure for Therapeutic Goods to resolve a problem with a therapeutic good already supplied in Australia for which there are issues, deficiencies or defects in relation to the safety, quality, efficacy (i.e. performance) or presentation of the good; (e) **advertising directions and prevention notices**: in instances of advertising non-compliance, the TGA may direct the advertiser to take steps to address the non-compliant advertising (e.g. ceasing the advertisement, making a correction or ceasing to make a particular claim); (f) **infringement notices**: if the TG Act has been breached, the TGA may issue an infringement notice. If the entity does not pay the infringement notice, the TGA may take further action (e.g. formal court action);

	(g) **enforceable undertakings**: as an alternative to court proceedings, the entity in breach of the TG Act may enter into a written agreement with the TGA, subject to approval by the Secretary of the Department of Health; (h) **injunctions**: the TGA can seek injunctions in the Federal Court or the Federal Circuit Court to: i) restrain an entity from contravening the TG Act; and ii) compel compliance with the TG Act or regulations if an entity refuses or fails to comply; (i) **civil penalties**: maximum civil penalties in the TG Act are 5,000 penalty units for an individual or 50,000 penalty units for a body corporate. One penalty unit is currently valued at AUD 313 under the Crimes Act 1914 (Cth); and (j) **criminal prosecutions**: criminal penalties can include between five to seven years imprisonment and fines of up to 4,000 penalty units for entities. In addition, under the Australian Consumer Law (Schedule 2 to the Competition and Consumer Act 2010 (Cth)), a consumer can seek compensation from a manufacturer who has supplied a product with a safety defect if that product has caused loss or damage, which includes: (a) injuries to the person making the claim or injuries or death to another individual; and (b) economic loss caused by damage to or destruction of another good, land, building or fixture. In determining whether a product has a safety defect, the court will consider: (a) the purposes for which the product has been marketed and how it was marketed; (b) product packaging; (c) the use of any mark in relation to the product; (d) instructions and warnings for assembly and use; (e) what might reasonably be expected to be done with the product; and (f) the time the product was supplied.

	Consumers may take the manufacturer responsible for the safety defect to court or make a complaint to a consumer protection agency.
Miscellaneous	
9. For summarising purposes, could you please list all the laws / regulations / guidelines and the relevant regulators in your jurisdiction that pertain to medical device cybersecurity?	Legislation: – Therapeutic Goods Act 1989 (Cth) – Privacy Act 1988 (Cth) – Security of Critical Infrastructure Act 2018 (Cth) – MyHealth Records Act 2012 (Cth) Regulations: – Therapeutic Goods (Medical Devices) Regulations 2002 (Cth) Other instruments: – Therapeutic Goods (Excluded Goods) Determination 2018 (Cth) Industry guidance: – Medical device cyber security guidance for industry by the Therapeutic Goods Administration of the Australian Department of Health and Aged Care dated November 2022 and accessible here.
10. For medical device cybersecurity, do you know any plans by local regulators to issue any specific rules, guidelines, or standards? What are the areas where regulations are most needed from your perspective?	To our knowledge, there are no current plans in Australia to issue new rules, guidelines or standards that specifically relate to medical device cyber security nor has there been any indication by the relevant authorities of reforming the existing regime. Australia's recent focus has been on national cyber security, critical infrastructure, and the minimisation of large-scale data breaches. On that front, the Australian Government issued the 2023-2030 Australian Cyber Security Strategy aimed at building sovereign capabilities against cyberattacks and ensuring that critical infrastructure is resilient and secure.

China

Latest update: August 2023

Definition and scope		
1.	In your jurisdiction, what is the legal definition for medical devices?	According to Regulation on the Supervision and Administration of Medical Devices (Revised in 2021), "medical devices" shall refer to the instruments, equipment, appliances, *in vitro* diagnostic reagents and calibrators, materials and other similar or relevant articles directly or indirectly used on the human body, including computer software needed; their utility are mainly obtained by physical or other means rather than by means of pharmacology, immunology or metabolism or, although such means are used, they only play a supplementary role; the purposes of medical devices are as follows: (1) the diagnosis, prevention, monitoring, treatment or relief of diseases; (2) the diagnosis, monitoring, treatment, relief or functional compensation of injuries; (3) the inspection, substitution, adjustment or support of physiological structures or physiological processes; (4) the support or maintenance of life; (5) the control of pregnancy; and (6) the provision of information for the purpose of medical treatment or diagnosis through the examination of a sample from a human body.
2.	(a) In your jurisdiction, are all types of health care related software (i.e., computer programs, applications, or systems specifically designed to support and enhance various aspects of healthcare delivery and management, including those in independent form and those attached to a physical	(a) Based on the above definition and Guiding Principles for Medical Device Software Registration Review, medical device software includes software that is itself a medical device (Software as a medical device, **SaMD**) or software that is included in a medical device (Software in a medical device, **SiMD**). - SaMD is software that has one or more medical purpose/use, does not require medical device

	medical device) can regarded as medical device based on the above definition? (b) If not all the health care related software can be covered by the definition of medical devices, is it clearly defined which kinds of medical related software will be regulated as a medical device and which are not?	hardware to fulfil its intended use, and runs on a general purpose computing platform; - SiMD is software that has one or more medical purpose/use, controls/drives medical device hardware or runs on a medical computing platform. (b) In addition to the above medical device software, medical-related software also includes other medical device software necessary for the normal operation of medical device software. Specifically, these include: - Essential software: other medical device software necessary for the normal operation of medical device software and medical middleware. - External software environment: the system software, common application software, common middleware, and support software that are necessary for the proper operation of medical device software. The essential software shall be registered separately as Medical Device Software. The external software environment does not include essential software and is not medical device software.
General regulatory requirements		
3.	For medical software that is regulated as a medical device ("**Medical Device Software**"), what regulatory steps (e.g., additional clinical trials, approvals, tests, maintenance, supplementary registration after software update) are required to be completed before it can be approved for market launch and during the post-marketing period?	i. Medical Device Software Clinical Evaluation Requirements Medical Device Software Clinical Evaluation Requirements According to the Guiding Principles for Medical Device Software Registration Review, the functions of medical device software are differentiated into "processing function" (including "pre-processing function" and "post-processing function"), "control function" and "safety function" from the perspective of technical characteristics, and "decision-making function" and "non-decision-making function" from the perspective of usage, and different clinical evaluation requirements are proposed for different types of software and functions of the software, including individual evaluation or overall evaluation, conducting clinical trials or analysing and evaluating

		the same varieties of medical devices through clinical literature, clinical data, etc. In general, SiMD is evaluated as a whole with the medical devices to which they belong, and some SiMD can be evaluated independently with reference to independent software. SaMD is usually evaluated clinically based on software functions, and clinical evaluation can be conducted based on software algorithms if necessary. The new core algorithms, core functions, and intended uses are in principle subject to clinical evaluation. The simple operation and pure process optimisation software functions can be evaluated through non-clinical evidence without clinical evaluation. For medical device software not exempted from clinical evaluation, it is necessary to distinguish between different types of software and software functions, and to choose different paths and clinical evidence for clinical evaluation.
	ii.	Medical Device Software Quality Assurance According to the Guiding Principles for Medical Device Software Registration Review, the main measures of software quality assurance include software testing, software verification, software validation, software configuration management, software defect management and software traceability analysis, etc. Among them: software testing is the basic measure of software quality assurance, while software traceability analysis needs to be carried out over the whole process of the software life cycle. Additionally, according to the Guiding Principles for Cybersecurity Registration Review of Medical Devices, when applying for registration, Medical Device Software is required to submit a cybersecurity study report and apply for a change of registration after a major software update.

Cybersecurity requirements

4.	Is Medical Device Software subject to general cybersecurity regulations in your jurisdiction? If so, (a) how do these regulations apply to Medical Device Software? (b) Can you provide a brief introduction of the general cybersecurity requirements that are applicable to the Medical Device Software?	(a)	In China, general cybersecurity regulations apply to network operators, which encompass the owners, administrators of networks, and network service providers. According to this definition, a network refers to a system composed of computers or other information terminals and related devices that collect, store, transmit, exchange, and process information based on specific rules and procedures. Considering this definition, the operation of Medical Device Software may fall under the scope of general cybersecurity regulations. During the operational phase, Medical Device Software is utilised to collect, store, transmit, exchange, and process information on the relevant computing platform/system.
		(b)	These requirements are in two parts—one is for organisational measures, and the other is for technical measures. Organisational measures requirements include requirements to formulate internal cyber security management rules and operating procedures, to have a data classification mechanism, and to assign responsible personnel to handle cybersecurity matters. Technical measures requirements include requirements to (i) adopt technical measures to prevent computer viruses and network attacks, network intrusion and other acts that endanger network security; (ii) take technical measures to monitor and record network operation status and network security events, and retain relevant network logs for not less than six months; and
		(c)	adopt measures such as important data backup and encryption.
5.	In addition to the generally applied cybersecurity requirements, are there any cybersecurity requirements that are specifically		Yes. For Medical Device Software, the National Medical Products Administration (**NMPA**) issued the Notice of on the Promulgation of Appendix to Good Manufacturing Practice for Standalone Software as Medical Devices, which applies to

	set for Medical Device Software, including any cybersecurity related requirements in its development, testing, deployment, and maintenance of Medical Device Software?	both standalone software and software components. According to this note, the key cybersecurity requirements for Medical Device Software are as follows: – Risk management activities shall be implemented throughout the software life cycle process, which shall take cybersecurity into account. – For software configuration management, control procedures shall be established and documented to standardise the control requirements for software versions, source codes, documents, tools and off-the-shelf software, and determine the requirements for configuration identification, change control, configuration status records and other activities. It is required to use configuration management tools to ensure software quality and run through the whole process of the software life cycle; – Software traceability analysis shall cover the controlling requirements for off-the-shelf software and cybersecurity. – Requirements for cybersecurity shall be included in the evaluation and use of off-the-shelf software. – Software verification activities like code review and testing shall cover cybersecurity verification requirements. – Software validation through user testing shall cover cybersecurity testing requirements. – Software update change control shall include cybersecurity change requirements. – Cybersecurity incidents shall be included in data analysis procedures. Emergency response plans for cybersecurity incidents shall be established. – Cloud computing agreements shall specify cybersecurity assurance requirements. The Guiding Principles for Cybersecurity Registration Review of Medical Devices (医疗器械网络安全注册审查指导原则) also imposes more detailed requirements on cybersecurity when reviewing the registration for the medical device. Among these requirements, one is worth noting. According to these principles, when cybersecurity updates affect the safety or effectiveness of a medical device (i.e. significant cybersecurity feature updates), the applicant of these medical devices must apply for a change in registration.

Data protection requirements	
6. How is data collected and processed by Medical Device Software regulated in your jurisdiction?	The processing of such data needs to comply with relevant provisions of the Data Security Law and the Personal Information Protection Law. Processing of device information that does not contain personal data needs to follow the Data Security Law, while the processing of personal information needs to comply with the Personal Information Protection Law. Additionally, if the processed data constitute human genetic resources (**HGR**) data (i.e. data derived from HGR materials), regulations on HGR data also need to be followed. China has also issued a recommended national standard Information Security Technology—Guide for Health Data Security, which while not mandatory, provides guidance on health data processing that can be followed as good practice.
7. Is there any data localisation requirement for the data generated or processed via the Medical Device Software?	Yes. There are a few regulations that impact data localisation requirements. When it comes to Medical Device Software, the following regulations and regulations are of relevance: 1. If the Medical Device Software user (i.e. the individual or entity that decides how to use the software, such as hospitals) meets one of the following conditions, it shall apply for and pass the security assessment by the regulator before exporting any data out of China: - if it constitutes a critical information infrastructure operator and transfers personal information out of China; - if it processes over one million natural persons' personal information; - if it exports accumulatively over 100,000 natural persons' personal information from 1 January of the preceding year; - if it exports accumulatively over 10,000 natural persons' sensitive personal information from 1 January of the preceding year; or - If it processes important data. Currently, the industry sectors are still in the process of formulating the catalogue of important data and the

	scope of important data is not clear at the current stage. 2. If the information generated by the Medical Device Software constitutes HRG data, before transferring such data out of China or sharing with a foreign entity, the Chinese data controller shall report to the Ministry of Technology and file the data with the Ministry of Technology.
8. From a compliance perspective, are the above regulatory requirements being fully implemented in practice? Are there any compliance risks that the Medical Device Software operators may need to note?	For cybersecurity-related requirements (e.g. when applying for the medical device registration), enterprises must draft the report on its cybersecurity and its evaluation. Subject to the regulator's review, significant importance is attached to these requirements and are largely followed. In practice, many Chinese companies are still in the process of implanting the requirements under the Personal Information Protection Law since it is a relatively new law in China. But since the life science sector is a heavily regulated sector, enterprises in this area are responding quickly to these requirements by modifying their internal management procedures and external privacy policies. In addition to the above, from a compliance perspective, the software operators should first clarify the scope of software to be included in the management of medical devices, avoiding the risks associated with marketing software that has the characteristics of a medical device without obtaining a medical device registration certificate. In the meanwhile, for software updates that may affect the safety and effectiveness of medical devices (i.e. major updates), operators should apply for a change of registration in a timely manner to avoid violating the requirements of the Regulation on the Supervision and Administration of Medical Devices.
Miscellaneous	
9. For summarising purposes, could you please list all the laws / regulations / guidelines and the relevant regulators in your jurisdiction that pertain to medical device cybersecurity?	The laws / regulations / guidelines are as follows: – PRC Cybersecurity Law (Effective on 1 June 2017); – Regulation on the Supervision and Administration of Medical Devices (Revised in 2021);

	– Notice of on the Promulgation of Appendix to Good Manufacturing Practice for Standalone Software as Medical Devices (Effective on 1 July 2020); – Guiding Principles for Cybersecurity Registration Review of Medical Devices (Revised in 2022); – Guiding Principles for Medical Device Software Registration Review (Revised in 2022); – Administrative Measures on the Registration and Record-filing of Medical Devices (Effective on 1 October 2021). The relevant regulators are as follows: – the National Medical Products Administration; – the State Administration for Market Regulation.
10. For medical device cybersecurity, do you know any plans by local regulators to issue any specific rules, guidelines, or standards? What are the areas where regulations are most needed from your perspective?	Based on the available public information, we are not aware of any specific rules, guidelines, or standards to be issued. Given that AI has been in rapid development in recent years and the increased use of AI in digital healthcare, we understand that documents such as special regulations for AI medical devices and their cybersecurity, and any special regulations for AI compared to general medical device software, will be needed.

India

Latest update: September 2023

Definition and scope		
1.	In your jurisdiction, what is the legal definition for medical devices?	Under the Medical Devices Rules, 2017 (**MDR**), enacted under the scope of the Drugs and Cosmetics Act, 1940 (**D&C Act**), medical devices are defined as being any of the below: (A) substances used for *in vitro* diagnosis and surgical dressings, surgical bandages, surgical staples, surgical sutures, ligatures, blood and blood component collection bag with or without anticoagulant; (B) substances including mechanical contraceptives (condoms, intrauterine devices, tubal rings), disinfectants and insecticides notified in official gazette of India; and (C) devices notified from time to time under the D&C Act.
2.	(a) In your jurisdiction, are all types of health care related software (i.e., computer programs, applications, or systems specifically designed to support and enhance various aspects of healthcare delivery and management, including those in independent form and those attached to a physical medical device) can regarded as medical device based on the above definition? (b) If not all the health care related software can be covered by the definition of medical devices, is it clearly defined which kinds of medical related software will be	(A) In India, software, whether used alone or in combination, intended by its manufacturer to be used specially for human beings or animals which does not achieve the primary intended action in or on human body or animals by any pharmacological or immunological or metabolic means, but which may assist in its intended function by such means for one or more of the specific purposes set out below are classified as 'medical device softwares' and fall under the scope of definition of medical devices - (i) diagnosis, prevention, monitoring, treatment or alleviation of any disease or disorder; (ii) diagnosis, monitoring, treatment, alleviation or assistance for, any injury or disability;

	regulated as a medical device and which are not?	(iii) investigation, replacement or modification or support of the anatomy or of a physiological process; (iv) supporting or sustaining life; (v) disinfection of medical devices; and (vi) control of conception. (B) Please see our response above. Further, note that medical devices, including medical device software (**MDS**), are regulated based on a risk-based classification approach. Accordingly, few software has been classified, and the list gets periodically updated.
General regulatory requirements		
3.	For medical software that is regulated as a medical device ("**Medical Device Software**"), what regulatory steps (e.g., additional clinical trials, approvals, tests, maintenance, supplementary registration after software update) are required to be completed before it can be approved for market launch and during the post-marketing period?	There are no specific additional regulatory steps for MDS before the same can be approved for market launch and during the post-marketing period. The same compliance is applicable to other medical devices, subject to their individual risk-based classification.
Cybersecurity requirements		
4.	Is Medical Device Software subject to general cybersecurity regulations in your jurisdiction? If so, (a) how do these regulations apply to Medical Device Software? (b) Can you provide a brief introduction of the general cybersecurity requirements that are	(A) Yes, companies offering services in relation to medical device software in India are subject to the cyber security and incident reporting direction issued by the Indian Computer Emergency Response Team (**CERT-In**) on 28 April 2022 (**CERT-In Direction**). The CERT-In Direction has a wide applicability and extends to body corporates (i.e. companies, including firms, sole proprietorships, or other association of individuals) engaged in commercial or professional activities in India. Considering the broad definition of body corporates, compliance under the CERT-In

	applicable to the Medical Device Software?	Direction will be required by companies engaged in the business of medical device software in India. (B) In respect of body corporates, the CERT-In Direction provides for the following key compliance: (i) Reporting mandatorily reportable cyber security incidents (as specified under the CERT-In Direction) to CERT-In within six hours of noticing or being brought to notice about such cyber security incidents; (ii) Synchronising and connecting the ICT system clocks with the network time protocol server of National Informatics Centre or National Physical Laboratory; (iii) Appointing a 'Point of Contact' and notifying to the CERT-In of such appointment; and (iv) Maintaining logs of ICT systems in India for a rolling period of 180 days.
5.	In addition to the generally applied cybersecurity requirements, are there any cybersecurity requirements that are specifically set for Medical Device Software, including any cybersecurity related requirements in its development, testing, deployment, and maintenance of Medical Device Software?	No such specific requirements exist under current Indian laws.
Data protection requirements		
6.	How is data collected and processed by Medical Device Software regulated in your jurisdiction?	In India, issues pertaining to privacy and data protection are dealt with by the Information Technology Act 2000 (**IT Act**) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (**SPDI Rules**). Hence, collection and processing of any data that is categorised as personal information (including sensitive personal data or information) will be governed by the IT Act and SPDI Rules.

	Compliance in relation to disclosure of personal information: While the IT Act does not prescribe compliance in relation to collection or processing of personal information, disclosure of personal information to third parties is subject to receipt of prior consent from the concerned information provider. Such consent can be obtained through any mechanism, since the manner of obtaining such consent has not been specified under the IT Act. Compliance in relation to sensitive personal data or information (**SPDI**): Personal information relating to the following has been designated as SPDI under the SPDI Rules: (i) password; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; and (vi) biometric information. Collection and processing SPDI are subject to compliance with the following key requirements: (i) implementation of reasonable security practices and procedures to protect SPDI by obtaining IS/ISO/IEC 27001 security certification; (ii) formulation and publication on the website of the body corporate, a privacy policy for handling of SPDI; (iii) obtaining written consent (or consent through electronic mode) from the information provider prior to collecting SPDI; (iv) appointing a grievance officer to address discrepancies/grievances relating to SPDI and publishing this officer's name and contact details on the website; (v) implementing a mechanism to delete/destroy SPDI once the purpose of its usage is over; and (vi) enabling information providers, the right to access/correct their SPDI and withdraw consent for the SPDI provided. Further, on 11 August 2023 the Digital Personal Data Protection Act 2023 (**DPDP Act**) was released as India's first comprehensive national legislation on data protection.

		However, the DPDP Act has yet to come into force. Once enforced, the DPDP Act will significantly enhance compliance requirements for protection of personal data of individuals.
7.	Is there any data localisation requirement for the data generated or processed via the Medical Device Software?	While there are no data localisation requirements on a sector neutral basis, the Health Data Management Policy 2020 should be taken into account. The Health Data Management Policy was approved by the Indian Government in December 2020. The aim of this policy is to create a framework for the secure processing of personal and sensitive personal data of individuals and is applicable to the entities involved in the Ayushman Bharat Digital Mission and the partners/persons who are a part of the National Digital Health Ecosystem. The scope of the Health Data Management Policy extends to medical device manufacturers as well. Subsequently, a revised Health Data Management Policy was published on 23 April 2022 (**Draft Revised Policy**). **The Draft Revised Policy provides that no personal data shall be stored beyond the geographical boundaries of India, subject always to the provision of applicable laws.** The Draft Revised Policy is still in a draft form and has yet to be formally rolled out by the Government.
8.	From a compliance perspective, are the above regulatory requirements being fully implemented in practice? Are there any compliance risks that the Medical Device Software operators may need to note?	There are no specific compliance risks under the general data protection laws in India. However, from a digital health perspective, some of the key issues faced by the industry are set out below: (A) lack of centrally mandated standards of data protection and security; (B) absence of proper education and training and public awareness for employees of any organisation who are responsible for collecting, processing and handling of customer/patient data; (C) while electronic health records guidelines (**EHR Guidelines**) were made public in 2016, they are not mandatory compliance, and compliance regarding management of patient health records remain largely voluntary.

Miscellaneous		
9.	For summarising purposes, could you please list all the laws / regulations / guidelines and the relevant regulators in your jurisdiction that pertain to medical device cybersecurity?	The cyber security and incident reporting direction issued by the Indian Computer Emergency Response Team on 28 April 2022, along with the IT Act, SPDI Rules, and the Intermediaries Guidelines 2011.
10.	For medical device cybersecurity, do you know any plans by local regulators to issue any specific rules, guidelines, or standards? What are the areas where regulations are most needed from your perspective?	We are not aware of any forthcoming plans regarding medical devices cybersecurity regulations in India. However, as the DPDP Act now awaits enforcement, it may be expected that in the near future, the regulations around medical device software and regulations specifically dealing with cybersecurity and data protection may be revisited. Regulatory guidance is desperately required for establishing uniform security standards. Further, with the boom of medical device software companies in the electronic health record/electronic medical record business, guidelines should essentially be replaced with statutorily mandatory compliance for robust data protection. Lastly, a comprehensive legal framework governing collection and dissemination of personal data, as well as concerns regarding data inaccuracy, bias, and/or discrimination is urgently required along with specific regulations for governing data collection and processing of non-sensitive personal data or information.

Indonesia

Latest update: October 2023

Definition and scope		
1.	In your jurisdiction, what is the legal definition for medical devices?	The Indonesian government has just enacted the new Law No. 17 of 2023 on Health ("Health Law") in August 2023, which replaces the previous law of 2009. Therefore, we expect that many implementing regulations will be enacted and put in place in the near future. Pursuant to the Health Law, a medical device is defined as an instrument, apparatus, machine, equipment, implant, reagent and *in vitro* calibrator, software, and materials thereof or similar thereto that are used for human medical purposes and do not achieve their main objective through pharmacology, immunology or the metabolic process. The Health Law also provides a definition for "medical technology", which includes all forms of equipment, products and/or methods intended to assist in establishing diagnoses, and the prevention and handling of human health problems. Furthermore, medical technology also includes hardware and software.
2.	(a) In your jurisdiction, are all types of healthcare-related software (i.e. computer programmes, applications, or systems specifically designed to support and enhance various aspects of healthcare delivery and management, including those in independent form and those attached to a physical medical device) regarded as medical devices based on the above definition? (b) If not all healthcare-related software can be covered by the	(a) Based on the definition in the Health Law, all types of healthcare-related software can be regarded as a medical device. In addition, pursuant to the Regulation of the Minister of Health No. 62 of 2017 on Product Licence of Medical Devices, In Vitro Diagnostic Medical Devices and Household Health Products ("MOH Regulation 62/2017"), it is also stipulated that medical devices include software. Therefore, it is safe to conclude that all types of healthcare-related software can be regarded as a medical device. (b) The types and names of medical devices can be referred to Decree of Minister of Health Decree No. 01.07 / Menkes/ 4745/ 2021 on Types and Naming of Medical Devices, which has classified the types and names of medical devices based

	definition of medical devices, which kinds of medical-related software will be regulated as a medical device and which are not?	on categories and sub-categories, which can be used by health facilities.
General regulatory requirements		
3.	For medical software that is regulated as a medical device ("Medical Device Software"), what regulatory steps (e.g. additional clinical trials, approvals, tests, maintenance, supplementary registration after software updates) must be completed before it can be approved for market launch and during the post-marketing period?	The MOH Regulation 62/2017 stipulates that every medical device, *in vitro* diagnostic medical device and household medical supplies must meet the following criteria before they are granted the relevant distribution permit: — Standard quality, in accordance with good production practice; — Safety and expediency thereof, which is proven by clinical trial results and/or other proof as may be necessary; — Dosage that does not exceed the limit determined in accordance with the prevailing standard, requirement and regulation; and — Does not use banned substances in accordance with the prevailing standard, requirement and regulation. In addition, in 2016 the Minister of Health also published a medical device licence module, which provides a guideline on the requirements to file for a medical device distribution licence ("License Module"). Pursuant to the Licence Module, the following five forms must be completed by applicants when applying for a medical device distribution licence: **Form A - Administration requirement** The documents that must be attached to Form A, among others, include the: (i) production certificate (issued by the Minister of Health to manufacturers who have implemented good medical device manufacturing methods to produce medical devices); (ii) medical device dealer licence; (iii) Letter of Authorisation (LOA) from the producer/principal; (iv) Certificate of free sale (CFS) (to explain that the medical device has obtained a distribution licence and is freely sold in the country of origin); (v) certificates and documents stating conformity of the medical device to product standards, requirements, safety requirements, effectiveness and quality

	systems in the design and manufacturing process (e.g. ISO 9001, etc.); (vi) executive summary; (vii) declaration of conformity (DoC); and (viii) trademark certificate. **Form B - Product information** This consists of, among others, a description of and the features of the medical device, general information, function, instruction for use, indication and counter-indication (if any), potential unwanted effects, materials, factory information, process of product, warnings and cautions (if any), and alternative therapy (if any). **Form C – Specification and quality assurance information** This consists of, among others, the functional characteristics and technical specification of the medical device, summary of the design verification and validation documents, pre-clinical trial (essential for class D medical devices), test results of software validation, clinical evidence, risk analysis (essential for class D medical devices), specifications and/or requirements of raw materials, test analyses/clinical test results of the safety of the medical device. **Form D – Instruction for use** **Form E – Post market evaluation** This consists of, among others, the handling of complaints from customers, product recalls, other information.
Cybersecurity requirements	
4. Is Medical Device Software subject to general cybersecurity regulations in your jurisdiction? If so, (a) how do these regulations apply to Medical Device Software? (b) Can you provide a brief introduction of the general cybersecurity requirements that are applicable to the Medical Device Software?	(a) Assuming that the medical device software will be processing data, then such device is subject to Indonesia's cybersecurity regulations pursuant to Law No. 11 of 2008 on Information and Electronic Transactions, which was amended by Law No. 19 of 2016 on Amendment to Law No. 11 of 1008 on Information and Electronic Transactions ("IET Law"). The IET Law does not specifically regulate medical software devices. However, it does stipulate provisions on electronic information and electronic transactions in general. The IET Law defines electronic information as one or a set of electronic data, including but not limited to texts, sounds,

	images, maps, photographs, electronic data interchange (EDI), electronic mail (email), telegrams, telex, telecopy, letters, signs, numbers, access codes, symbols, or perforations that have been processed that carry meaning or may be understood by persons qualified to understand them. The IET Law also defines an electronic system as a set of electronic equipment and procedures, which has the function to prepare, collect, process, analyse, store, display, publish, deliver and/or disseminate electronic information. While electronic system operator is defined as any persons, state administrators, business entities, and members of the public who provide, manage and/or operate an electronic system individually or collectively to electronic system users for their own interests and/or the interests of other parties. Additionally, Regulation of the Minister of Communications and Informatics No. 5 of 2020 on Private Electronic System Operators ("MOCI Regulation No.5/2020") stipulates that operating an electronic system in the private sector means the operation of electronic system by persons, business entities and members of the public. Since a medical device software contains electronic information and processes such electronic information, then the operation thereof is subject to the IET Law and MOCI Regulation No.5/2020. (b) The general cybersecurity requirement in the IET Law is stipulated in Article 15 whereby the operator of an electronic system must operate this electronic system reliably, safely and responsibly. Furthermore, Article 16 of the IET Law stipulates that if it is not provided for by another law in specific field of business, each electronic system operator must operate an electronic system with the following minimum requirements: — It re-displays electronic information and/or electronic documents in whole in accordance with the relevant retention period determined by the relevant law and regulation; — It can protect the availability, integrity, authenticity, secrecy and accessibility of electronic information in the operation of such electronic system;

	— It can be operated in accordance with the procedures or guidelines set out for operating such electronic system; — It is equipped with procedures or guidelines published in a language and with information or symbols that can be understood by parties relevant to the operation of such electronic system; and — It shall incorporate a mechanism to ensure the ongoing updates, clarity, and accountability of associated procedures or guidelines. In addition, MOCI Regulation No.5/2020 also stipulates that all private electronic system operators who fulfil the criteria listed below must register with the Minister of Communication and Information Technology before the relevant electronic system can be used: i. provide, manage, and/or operate offers and/or trade of goods and/or services (e.g. marketplace, e-commerce platforms); ii. provide, manage, and/or operate financial transaction services (e.g. financial technology, payment gateway platforms); iii. deliver paid digital material or content through the data network by means of download via a portal or website, e-mail, or via other applications to the user's device (e.g. paid on-demand services such as OTT platforms); iv. provide, manage and/or operate communication services including but not limited to short messages, voice calls, video calls, e-mail, and online conversations in the form of digital platforms, networking services and social media (e.g. social media platforms); v. provide search engine services, services for providing electronic information in the form of writing, sound, images, animation, music, video, films and games or a combination of part and/or all of them (e.g. Google search); and/or vi. process personal data for public service operational activities that are related to electronic transaction

	activities (i.e. any platform that involves personal data in order to facilitate electronic transaction). In relation to cybersecurity, pursuant to Government Regulation No. 71 of 2019 on Electronic System and Transaction Operations ("GR No.71/2019"), electronic system operators are required to: — have and run procedures and facilities securing its electronic system in order to avoid any disruptions, failures and losses; — provide a security system that covers procedures and systems for the prevention and overcoming of threats and attacks that result in any disruptions, failures and losses; and — in the occurrence of a system failure or disruption that brought about serious impact on an electronic system as a result of actions by other party, the electronic system operator must secure electronic information and/or electronic documents and immediately report (at the first instance) such occurrence to law enforcement officials and related ministries or agencies.
5. In addition to the generally applied cybersecurity requirements, are there any cybersecurity requirements that are specifically set for Medical Device Software, including any cybersecurity related requirements in the development, testing, deployment, and maintenance of Medical Device Software?	The Health Law does not stipulate any specific provision on requirements related to medical device software.
Data protection requirements	
6. How is data collected and processed by Medical Device Software regulated in your jurisdiction?	In Indonesia, Personal Data Protection is stipulated under Law No. 27 of 2022 ("PDP Law"). The PDP Law defines personal data protection as a comprehensive effort to protect personal data in processing of personal data to guarantee the constitutional rights of personal data subjects. Pursuant to the PDP Law, the processing of personal data includes:

	a. obtaining and collecting; b. managing and analysing; c. storing; d. correcting and updating e. displaying, publishing, transferring, disseminating or disclosing; and/or f. deleting or destroying of personal data. The processing of personal data must be done in accordance with the following principles of personal data protection: — the collection of personal data is done within limitations and that it is specific, lawful and transparent; — the processing of personal data is done in accordance with its purpose; — the processing of personal data is done by ensuring the rights of personal data subjects; — the processing of personal data is done accurately, completely, has not been misleading, is up to date and is accountable; — the processing of personal data is done by protecting the security of personal data from unauthorised access, unauthorised disclosure, unauthorised alteration, misuse, destruction and/or erasure of personal data; — the processing of personal data is done by informing the purposes and activities of processing and failure to protect personal data; — the record of personal data is destroyed and/or deleted after the expiration of the retention period or based on the request of personal data subject, unless stipulated otherwise by the relevant laws and regulations; — the processing of personal data is done responsibly and transparently. Processing of personal data may also be carried out in public places or in public service facilities by installing data processing or processing equipment. However, the processing of personal data in public places may only be carried out for the purposes of security, disaster prevention,

		and/or traffic organisation or the collection, analysis, and regulation of traffic information. It is not used to identify a person and must display information in the area where the visual data processor is installed. Processing of personal data may be carried out by two or more personal data controllers. These personal data controllers are individuals, public bodies and international organisations acting individually or collectively. Then, the personal data controller must fulfil requirements, such as: there must be an agreement between the personal data controllers pertaining to the roles, responsibilities, and relationships between the personal data controllers; there must be interrelated purposes and a jointly determined way of processing personal data; and there must be a jointly appointed contact person. The Health Law also stipulates provisions on the protection of personal data and information in relation to the health information system. In this regard, health information system organisers must ensure the protection of health data and the information of each individual. The processing of health data and information that uses an individual's health data requires the consent of the data owner and/or the fulfilment of other provisions, which are the basis for the processing of personal data in accordance with the provisions of laws and regulations in the field of personal data protection.
7.	Is there any data localisation requirement for data generated or processed via the Medical Device Software?	There are no specific regulation pertaining to localisation requirement for data generated or processed by medical device software. However, the PDP Law stipulates that the controller of personal data may transfer personal data to another controller and/or processor of personal data outside Indonesia. In conducting such transfer of personal data outside of Indonesia, the transferor must ensure that the country where the transferee resides has a personal data protection measure equal to or higher than the measures stipulated in the PDP Law. If such measures do not exist, then the transferor must ensure that adequate and binding personal data protection measures exist between the parties involved.

8.	From a compliance perspective, are the above regulatory requirements being fully implemented in practice? Are there any compliance risks that the Medical Device Software operators may need to note?	All regulatory requirement pertaining to electronic system operators and medical devices are being fully implemented, although we expect some changes due to the recently enacted Health Law. As to the regulatory requirements set out in the PDP Law, the full implementation thereof is still pending because the PDP Law provides a grace period of two years as of its enactment date for all stakeholders to make all necessary adjustments pursuant to the PDP Law. Non-compliance of the prevailing laws and regulations carries the risk of administrative sanction (e.g. revocation of a licence) and criminal prosecution (e.g. imprisonment and/or penalties).
Miscellaneous		
9.	For summarising purposes, could you please list all the laws / regulations / guidelines and the relevant regulators in your jurisdiction that pertain to medical device cybersecurity?	The following is a list of regulations that are relevant to medical device cybersecurity: a. Law No. 17 of 2023 on Health; b. Regulation of Minister of Health No. 62 of 2017 on Product Licence of Medical Devices, In Vitro Diagnostic Medical Devices and Household Health Products; c. Decree of Minister of Health No. 01.07 / Menkes/ 4745/ 2021 on Types and Naming of Medical Devices; d. Law No. 11 of 2008 as amended by Law No. 19 of 2016 on Information and Electronic Transactions; e. Government Regulation No. 71 of 2019 on Electronic System and Transaction Operations; f. Regulation of the Minister of Communications and Informatics No. 5 of 2020 on Private Electronic System Operators; g. Law No. 27 of 2022 on Personal Data Protection.
10.	For medical device cybersecurity, do you know any plans by local regulators to issue any specific rules, guidelines, or standards?	As of now, we are not aware of any immediate plans by the government to issue any specific regulations pertaining to medical device cybersecurity.

	What are the areas where regulations are most needed from your perspective?	

Japan

Latest update: August 2023

Definition and scope	
1. In your jurisdiction, what is the legal definition for medical devices?	In Japan, the legal definition for medical devices is stipulated in the "Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices" (**PMD Act**) and its enforcement regulations and cabinet orders as follows: • Medical appliances or instruments, etc. which are intended for use in the diagnosis, treatment or prevention of disease in humans or animals, or intended to affect the structure or functioning of the bodies of humans or animals (excluding regenerative medicine products), and which are specified by Cabinet Order Article 2, paragraph 4 of the PMD Act (hereinafter, abbreviated as the **Act**). • Medical appliances or instruments, etc. refer to medial appliances or instruments, dental materials, medical supplies, sanitary goods, and programmes, and recording media on which programmes are recorded (Article 2, paragraph 1, item (ii) of the Act). • Programmes refer to a combined set of instructions given to a computer in order to produce a certain result (same item above). • The Appendix of the Cabinet Order comprehensively lists items that may fall under medical devices, and most of the medical appliances and instruments, etc. that are intended to be used for diagnosis of diseases, etc., or to affect the structure of the body, etc., would fall under the Appendix. However, masks, for example, are not included in the Appendix, so even medical masks are not considered medical devices. Therefore, it is necessary to check the Appendix when determining the applicability of medical devices, etc.

		• Under the PMD Act, medical devices are classified into the following categories in descending order of health-risk level in the event of functional impairment, etc.: (1) Medical devices that may have a serious effect on human life and health: Specially-controlled medical devices (Class IV/III); (2) Medical devices that may have an effect on human life and health: Controlled medical devices (Class II); (3) Medical devices with little or no effect on human life and health: General medical devices (Class I); This classification under the PMD Act is based on the classification rules of the Global Harmonisation Task Force (GHTF) and is basically internationally unified.
2.	(a) In your jurisdiction, are all types of health care related software (i.e., computer programs, applications, or systems specifically designed to support and enhance various aspects of healthcare delivery and management, including those in independent form and those attached to a physical medical device) can regarded as medical device based on the above definition? (b) If not all the health care related software can be covered by the definition of medical devices, is it clearly defined which kinds of medical related software will be regulated as a medical device and which are not?	Not all healthcare-related software falls under the above definition of medical devices, and Class I is excluded. • A medical device programme is a programme that has a purpose that meets the definition of medical devices, such as contributing to the diagnosis, treatment, or prevention of disease, and is used for giving general-purpose computers such as a desktop computers or portable information terminals such as smartphones (hereinafter referred to as **General-Purpose Computers**) additional functions as medical devices by installing such programmes. The determination of whether this applies or not is based on (1) whether the purpose of using the programme is to diagnose, treat, or prevent disease or not (see A1 above), and (2) the degree of health risks in the event of a defect in the programme. • With regard to (2) above, a programme that has a low degree of both contribution to the diagnosis of disease, etc. (contribution) and low risk of harm to human life and health in the event of untoward effects or malfunction of the programme (risk), is classified as Class I, and regardless of the intended use of (1) above, such programmes are not classified as medical devices. (Article 1 of the Cabinet Order, Appendix 1).

	• More specifically, we can refer to the Ministry of Health, Labour and Welfare's notification titled "Basic Idea on whether Programmes fall under Medical Devices," and the categorisation can be organised as follows. A: Programmes that fall under medical devices: i. Programmes that process data (including images) obtained from medical devices to create indicators, images and graphs, etc., for use in diagnosis or treatment; ii. Programmes that assist in determining treatment plans and methods (including simulations). B: Programmes that do not fall under medical devices: i. Programmes that transfer, store or display data obtained from medical devices for use as diagnostic records; ii. Programmes for processing data (excluding images) (excluding those used for diagnosis); iii. Educational programmes; iv. Programmes for providing explanation to patients; v. Programmes for maintenance; vi. In-Hospital operations support programmes; vii. Health care management programmes; viii. Programmes equivalent to general medical devices (those that have little or no risk of affecting human life and health in the event of malfunctions, etc.).
General regulatory requirements	
3. For medical software that is regulated as a medical device ("**Medical Device Software**"), what regulatory steps (e.g., additional clinical trials, approvals, tests, maintenance, supplementary registration after software update) are required to be completed before	• In order to manufacture and market medical devices, approval, certification or notification is required for the relevant item. Certification by a registered certification body is required to market Class II and III medical devices (Article 23-2-23, paragraph 1 of the Act), and approval is required to manufacture and market Class

it can be approved for market launch and during the post-marketing period?	IV medical devices (Article 23-2-5, paragraph 1 of the Act). • Approval system: Based on the application materials submitted by the applicant for approval (including materials concerning test results of clinical trials), the examination authority exams the purpose, effect, form, structure, principle, raw materials, performance and safety specifications, method of use, storage method, validity period, and defects of the medical device. The quality, efficacy and safety of the medical device as a product are determined from the perspective of the benefit-risk balance of using the device (Article 23-2-5, paragraph 2, item (iii) of the Act, and the first sentence of paragraph 6 of the said Article). All approvals are granted by the Minister of Health, Labour and Welfare (Article 23-2-5, paragraph 1 of the Act), and the approval review is conducted by the Pharmaceuticals and Medical Devices Agency (PMDA) (Article 23-2-7, paragraph 1 of the Act, Article 37-29 of the Cabinet Order). • Certification system: Unlike "approval," which requires individual examination for efficacy and safety, certification is conducted to verify that medical devices subject to specified standards designated by the Minister of Health, Labour and Welfare conform to such standards or not, and can be conducted in a shorter time than the approval process. Certification is granted by a certification body (registered certification body) registered by the Minister of Health, Labour and Welfare (Article 23-2-13 of the Act). When applying for certification, the applicant is required to attach materials showing that the medical device subject to the application conforms to the certification standards and the basic requirements standards (Article 41, paragraph 3 of the Act). • Common matters:

	In order to receive approval and certification, the following requirements must be met in addition to the above determination of efficacy and safety. — The applicant for approval and/or certification must have a license of manufacturing and marketing (Article 23-2, paragraph 1 of the Act). — The manufacturing facility that manufactures medical devices must be registered as a manufacturing business (Article 23-2-3, paragraph 1 and Article 23-2-4 of the Act and Article 23-2-5, paragraph 2, items (i) through (iii) of the Act). — In the series of manufacturing processes of medical devices, appropriate manufacturing control and quality control must be implemented, and a system must be in place to manufacture medical devices in accordance with the approved contents, etc. (Article 23-2-5, paragraph 2, items (iv) and (v) of the Act). The QMS Ministerial Order establishes standards for such manufacturing and quality control of medical devices. After approval, a document-based or on-site investigation (hereinafter referred to as **QMS Conformity Investigation**) is conducted periodically (every five years) (Article 23-2-5, paragraph 7 of the Act, Article 37-21 of the Cabinet Order).
Cybersecurity requirements	
4. Is Medical Device Software subject to general cybersecurity regulations in your jurisdiction? If so, (a) how do these regulations apply to Medical Device Software? (b) Can you provide a brief introduction of the general cybersecurity requirements that are	• The Basic Act on Cybersecurity is a comprehensive act regarding information security. The said Act provides for the basic principles and matters regarding cybersecurity measures of our country, and clarifies the responsibilities of the national government. However, the said Act does not provide for specific individual requirements, etc., for business operators including those regarding medical-device programmes.

	applicable to the Medical Device Software?	• Under the Basic Act on Cybersecurity, the government requests business operators in the field of critical infrastructure to enhance their cybersecurity measures. In the medical sector in the field of critical infrastructure, medical institutions are considered critical infrastructure business operators. The government has also issued a number of notifications regarding the measures against cyber security problems medical institutions and medical device business operators should take, requesting them to implement technical security measures, etc., including cybersecurity measures.
5.	In addition to the generally applied cybersecurity requirements, are there any cybersecurity requirements that are specifically set for Medical Device Software, including any cybersecurity related requirements in its development, testing, deployment, and maintenance of Medical Device Software?	• The Ministry of Health and Welfare has formulated "Security Guidelines for Medical Data Systems" applicable to all information systems handling medical data. These guidelines specify security control measures listed below including those falling under the definition of the medical device programmes (see A2 above): — As internal control for the operation and use of medical data system, (1) formulation of basic policies and plans regarding organisational security control, etc., (2) development of a system necessary for security control, etc., (3) formulation of security control rules in the organisation, and (4) operation in accordance with the above; — risk assessment and control; — restrictions on use; — selection of a medical data system service provider appropriate as an outside data storage service provider; — creation of backups; and — detection, blocking and monitoring of unauthorised communications (zero trust approach). • Administrators of hospitals or clinics are required to take the measures necessary to ensure cybersecurity

	so that the provision of medical care will not be significantly hindered (Article 14, paragraph 2 of the Enforcement Regulations on the Medical Care Act). • The Ministry of Health, Labour and Welfare has issued a notification titled "Ensuring cybersecurity of medical devices." This notification asks for the appropriate management of cyber risks related to medical devices in order to ensure the safe usage of medical devices, based on the basic requirement standards for the certification system under the PMD Act (see A3 above). • In March 2023, the Ministry of Health, Labour and Welfare established medical device cybersecurity development goals and evaluation standards incorporating the guidance of the International Medical Device Regulators Forum (IMDRF), and amended the basic requirement standards, etc., which came into force in May 2023 (a period for transitional measures has been placed until June 30, 2024). By doing this, the Ministry of Health, Labour and Welfare confirms the measures against cyber security problems in the process of granting the permissions and licenses of medical devices. • The primary guidelines indicating specific cybersecurity measures for medical devices include the "Security Guidelines for Medical Data Systems" and those listed below: — Guidebook on introduction of medical device cybersecurity; — Guidebook on ensuring medical device cybersecurity at medical institutions; and — Guidelines for security control at information system service providers handling medical data (Ministry of Internal Affairs and Communications/Ministry of Economy, Trade and Industry).

Data protection requirements	
6. How is data collected and processed by Medical Device Software regulated in your jurisdiction?	There are no regulations that are individually applicable to "data collected and processed by medical device software", which is governed by the following general laws and regulations: 1. Regulations under the Act on the Protection of Personal Information: Data collected and processed by medical device software may fall under the definition of personal information or sensitive personal information under the Act on the Protection of Personal Information (**APPI**). **Personal Information** means information related to existing individuals that "can identify a specific individual by personal name, date of birth, or any other descriptions, etc. included in such information (including any information which can be easily cross-checked against any other information, enabling identification of a specific individual)" or "containing an Individual Identification Code" (Article 2, paragraph 1, items (i) and (ii) of the APPI). • The overview of the regulations applicable to Personal Information are as listed below: — When processing personal information, the purpose of use must be specified (Article 17, paragraph 1 of the APPI). — Personal Information must not be processed beyond the scope of the purpose of use without the consent of the relevant individual or a cause set forth under the relevant law or regulation (Article 18, paragraph 1 of the APPI). — Personal Information must not be used in an inappropriate manner that would encourage or induce illegal or unfair acts, etc. (Article 19, of the APPI).

	— Personal Information must not be acquired through false or any other unauthorised manner (Article 20, paragraph 1 of the APPI). — The purpose of use must be disclosed to the public in advance or notified at the time of acquisition (Article 21 of the APPI). • Further, any Personal Information constituting a Personal Information database is called **Personal Data** (Article 2, paragraph 3 of the APPI), to which the following regulations apply: — Efforts must be made to ensure the accuracy of Personal Data (Article 22 of the APPI). — Efforts must be made to delete any unnecessary Personal Data (Article 22 of the APPI). — Security control measures must be taken (Articles 23 to 25 of the APPI). — Data breach must be reported to the Personal Information Protection Commission and the affected individuals (Article 26 of the APPI). — Personal Information must not be provided to any third party without the consent of the relevant individual or a certain cause (Article 27, paragraph 1 of the APPI). — Personal Information must not be provided to any third party in a foreign country unless (1) the consents of the relevant individuals are obtained, or (2) the recipient has a system conforming to standards in place (Article 28 of the APPI). For the avoidance of doubt, (3) such foreign country does not include EU or United Kingdom (Personal Information Protection Commission Notification No. 1 of 2019). — When providing Personal Information to a third party, the matters provided in the APPI must be confirmed or recorded (Articles 29 and 30 of the APPI).

	• **Sensitive Personal Information** means Personal Information relating to an identifiable person's race, creed, social status, medical history, criminal record, the fact of having suffered damage by a crime, or other identifiers or their equivalent prescribed by Cabinet Order as those of requiring special care so as not to cause unjust discrimination, prejudice or other disadvantages to that person" (Article 2, paragraph 5 of the APPI). Regulations stricter than those applicable to personal information provided above are imposed on the acquisition and provision of Sensitive Personal Information. — Consent of the relevant individuals must be obtained when acquiring Sensitive Personal Information] (Article 20, paragraph 2 of the APPI). — Except as set forth in Article 20, paragraph 2 of the APPI, Sensitive Personal Information must not be provided to any third party unless the consent of the relevant individuals is obtained (excluding opt-out consents). 2. Regulations under the Next Generation Medical Infrastructure Act: The Next Generation Medical Infrastructure Act (**NGMIA**) develops a mechanism for utilisation of so-called medical big data such as Databases and Similar Collections of Anonymised Medical Data which is a collection of information including **Anonymised Medical Data** meaning information related to individuals, which is anonymised **Medical Data** (i.e. information regarding the medical history and mental or physical conditions of specific individuals as per Article 2, paragraph 1 of the NGMIA) so that specific individuals cannot be identified, and made unrestorable (Article 2, paragraph 3 of the NGMIA). Utilisation of Medical Data collected by Medical Device Software may be subject to regulations under the NGMIA.

	• The overview of the regulations under the NGMIA are as listed below: — Business operators generating Anonymised Medical Data shall obtain approval from the competent minister by application (Article 8 of the NGMIA; such approved business operator generating Anonymised Medical Data shall be hereinafter referred to as an **Approved Business Operator**). An Approved Business Operator may engage only Approved Business Operators to handle all or part of the Medical Data, etc., or Anonymised Medical Data it manages in relation to its approved business (Article 23, paragraph 1 of the NGMIA). — An Approved Business Operator may collect Medical Data based on which Anonymised Medical Data is generated only from other Approved Business Operators and business operators handling Medical Data (e.g. hospitals) (Article 25, paragraph 1 and Article 30, paragraph 1 of the NGMIA). However, an Approved Business Operator must not, subject to certain exceptions, handle such medical data beyond the scope necessary for its approved business (Article 17 of the NGMIA), and when generating Anonymised Medical Data, it must process such Medical Data so that specific individuals cannot be identified and that the Medical Data to be used for such generation cannot be restored in accordance with laws and regulations (Article 18, paragraph 1 of the NGMIA), and when handling such Anonymised Medical Data, it must not cross-check such Anonymised Medical Data with other information in order to identify the individuals related to the Medical Data used for generating such Anonymised Medical Data (Article 18, paragraph 2 of the NGMIA). — Anyone who receives Anonymised Medical Data and wishes to utilise the same (**Handling Business Operator**) must consult with an

		Approved Business Operator in advance, and go through a screening process by the screening committee established within the Approved Business Operator. — An Approved Business Operator and a Handling Business Operator shall enter into an agreement regarding the provision and receipt of Anonymised Medical Data, and ensure by such agreement that the manner of use of such Anonymised Medical Data and the related security control measures are appropriate. — A Handling Business Operator must not, in order to identify the individuals related to the Medical Data used to generate the Anonymised Medical Data it has received, acquire any descriptions or individual identification codes deleted from such Medical Data, or any information regarding the manner of processing, or cross-check such anonymised medical data with other information (Article 18, paragraph 3 of the NGMIA).
7.	Is there any data localisation requirement for the data generated or processed via the Medical Device Software?	There are no clear regulations regarding data localisation. However, as stated above, the APPI provides that Personal Data must not be provided to any third party in a foreign country (excluding EU and United Kingdom) unless (1) the informed consent of the relevant individuals are obtained, or (2) the recipient has systems in place conforming to standards (Article 28 of the APPI). The NGMIA also provides that any corporation without the principal place of business in Japan but handles Medical Data, etc., or Anonymised Medical Data in a foreign country can be an Approved Business Operator (Article 15 of the NGMIA). Therefore, it is considered that the NGMIA does not provide for data localisation.
8.	From a compliance perspective, are the above regulatory requirements being fully implemented in practice? Are there any compliance risks that	1. Act on the Protection of Personal Information: As the amended APPI was just enforced on 1 April 2022, it is likely that some companies have yet to revise their personal information protection rules and privacy policies and develop

	the Medical Device Software operators may need to note?	their internal systems. However, it is our understanding that companies are taking steps to address this situation from the standpoint of compliance. The APPI provides for the collection of reports and on-site inspections (Article 146 of the APPI) and guidance and advice (Article 147 of the APPI) by the Personal Data Protection Commission. In addition, violations of the APPI may result in recommendations and orders by the Personal Data Protection Commission (Article 148 of the APPI). Further, violations of an order may result in a public announcement to that effect (Article 148, paragraph 4 of the APPI) and a penalty of up to 100 million yen (Article 178, and Article 184, paragraph 1, item (i) of the APPI). The above outlines the compliance risks for businesses. 2. Next Generation Medical Infrastructure Act The number of Approved Business Operators under the NGMIA is still small, and regulatory requirements are considered to be strictly adhered to. The NGMIA provides for on-site inspections (Article 35 of the NGMIA) and guidance and advice (Article 36 of the NGMIA) by the competent minister. In addition, violations of the NGMIA may result in a rectification order (Article 37 of the NGMIA). Further, violations of an order may result in a fine of up to JPY 100 million (Article 46, item (iv), Article 49, paragraph 1, item (i) of the NGMIA). The above outlines the compliance risks for businesses.
Miscellaneous		
9.	For summarising purposes, could you please list all the laws / regulations / guidelines and the relevant regulators in your jurisdiction that pertain to medical device cybersecurity?	1. Laws and Regulations: • Act on the Protection of Personal Information, and enforcement regulations and cabinet orders incidental thereto. • Next Generation Medical Infrastructure Act, and enforcement regulations and cabinet orders incidental thereto. • Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical

	Devices, and enforcement regulations and cabinet orders incidental thereto. • Medical Care Act, and enforcement regulations and cabinet orders incidental thereto. 2. Guidelines: • Guidelines on the Act on the Protection of Personal Information (General Rules). • Guidelines on the Act on the Protection of Personal Information (Provision to Third Parties Located Overseas). • Guidelines on the Act on the Protection of Personal Information (Confirming Provision to Third Parties, and Obligation to Record). • Guidelines on the Act on the Protection of Personal Information (Pseudonymised Personal Information, and Anonymised Personal Information). • Guidance for the Appropriate Handling of Personal Information by Medical and Nursing Care-Related Businesses. • Guidelines on the Next Generation Medical Infrastructure Act. • Guidelines related to medical device applicability to programmes. • Guidebook on ensuring medical device cybersecurity at medical institutions. • Security guidelines for medical data systems. • Ensuring cybersecurity of medical devices. • Guidance on ensuring cybersecurity of medical devices. • Publication of IMDRF guidance. • Guidebook concerning the ensuring and thorough enforcing the of cybersecurity of medical devices. • Guidelines for security control at information system service providers handling medical data. 3. Regulatory Authority:

	• Ministry of Health, Labour and Welfare Matters related to approving the marketing of medical device programmes. • Personal Information Protection Commission Matters related to personal information (including sensitive personal information) that will be obtained or processed using medical device programmes. • Cabinet Office Administrative Jurisdiction of the Next Generation Medical Infrastructure Act. • Ministry of Internal Affairs and Communications Administrative jurisdiction of policy on Cybersecurity Matters related to safety control by providers of information systems and services that handle medical data. • Ministry of Economy, Trade and Industry Matters related to safety control by providers of information systems and services that handle medical data.
10. For medical device cybersecurity, do you know any plans by local regulators to issue any specific rules, guidelines, or standards? What are the areas where regulations are most needed from your perspective?	There does not seem to be such a plan at this time. Since leaks of medical data can cause irreparable damage to the data subject, strict regulations must be established for its handling. Dramatic advances in medicine, such as curing intractable diseases, can be expected if medical data can be utilised while maintaining anonymity. Therefore, from such perspective, we believe that regulation is necessary to find a balance between the utilisation of medical data and protecting anonymity. In this regard, after considerations were made for a new system of anonymisation suited to the actual conditions of research and development in the medical field, the NGMIA was amended in May 2023 to include the concept of Pseudonymised Medical Data, to enable data to be provided under the strict control of Approved Business Operators. The operational status of NGMIA will be the focus of attention in the future.

Korea

Latest update: August 2023

Definition and scope	
1. In your jurisdiction, what is the legal definition for medical devices?	Article 2(1) of the Medical Devices Act defines "medical device" as an instrument, machine, apparatus, material, software, or any other similar product for human beings or animals used independently or in combination for the purposes specified in the following subparagraphs, provided that drugs and quasi-drugs under the Pharmaceutical Affairs Act and the prosthetic limbs and aids among assistive devices for persons with disabilities under Article 65 of the Act on Welfare of Persons with Disabilities shall be excluded herefrom: 1. A product used for the purpose of diagnosing, curing, alleviating, treating, or preventing a disease; 2. A product used for the purpose of diagnosing, curing, alleviating, or correcting an injury or impairment; 3. A product used for the purpose of testing, replacing, or transforming a structure or function; or 4. A product used for the control of conception.
(a) In your jurisdiction, are all types of health care related software (i.e., computer programs, applications, or systems specifically designed to support and enhance various aspects of healthcare delivery and management, including those in independent form and those attached to a physical medical device) can regarded as medical device based on the above definition?	As mentioned above, the Medical Devices Act provides “software” as a type of medical devices. To be specific, under the Regulations on the Approval, Reporting, and Review of Medical Devices (**Regulations on Medical Devices**), “Medical Device Software” is defined as software, including embedded software, stand-alone software, and mobile medical apps, developed and manufactured for the purposes stipulated in Article 2 of the Medical Devices Act, which are listed in Section 1 above. In addition, software that transmits data generated by medical devices to a server to store, analyse, and process signals and images are also included in

2. (b) If not all the health care related software can be covered by the definition of medical devices, is it clearly defined which kinds of medical related software will be regulated as a medical device and which are not?	the scope of Medical Device Software (Article 2(2)) of the Regulations on Medical Devices). The Guidelines on the Approval and Review of Medical Device Software (**Guidelines on Medical Devices Software**) issued by the Ministry of Food and Drug Safety, stipulating specific matters regarding Medical Device Software approval and assessment, state that firmware-level software that controls medical devices without a separate display or user screen, software used for manufacturing and development of medical devices, and software used for quality management of medical devices such as purchasing and management programmes are excluded from the scope of Medical Device Software. Given the above definition, if software is developed and manufactured for the aforementioned purposes, such software will be regarded as a medical device.
General regulatory requirements	
3. For medical software that is regulated as a medical device ("**Medical Device Software**"), what regulatory steps (e.g., additional clinical trials, approvals, tests, maintenance, supplementary registration after software update) are required to be completed before it can be approved for market launch and during the post-marketing period?	The Medical Device Act stipulates various types of business (e.g. manufacturing, importing, repair, distribution or lease) related to the Medical Device and the required regulatory steps differ based on the types. 1. Medical device manufacturing business (Articles 6, 7) • A person who intends to engage in the business of manufacturing medical devices ("manufacturer") must obtain manufacturing business approval from the Ministry of Food and Drug Safety. When filing an application for manufacturing business approval, the applicant must also file an application for manufacturing approval, manufacturing certification, or manufacturing report for at least one item. Moreover, any person who intends to obtain manufacturing business permission must employ a quality manager. • The manufacturer must obtain manufacturing approval, certification, or report of the medical device it intends to manufacture. The type of licence differs based on the possible risk that may be caused in case of failure or malfunction. The manufacturer must be equipped with the necessary facilities and

	manufacturing and quality control systems before filing an application. The manufacturer must also submit necessary information, such as information on manufacturing and quality control systems, technical documents, and clinical trial data, to the Ministry of Food and Drug Safety. • The Ministry of Food and Drug Safety may grant manufacturing business approval, manufacturing approval, or manufacturing certification, or receive a manufacturing notification on condition that an applicant be equipped with facilities and manufacturing and quality control systems within a specified period. 2. Medical device import business (Article 15) • A person who intends to engage in the business of importing medical devices ("importer") must obtain import business permission from the Ministry of Food and Drug Safety. When filing an application for import business approval, the applicant shall file together an application for import approval, import certification, or import notification on at least one medical device to be imported. • An importer with import business approval shall obtain import approval, import certification, or file an import report with regard to medical devices intending to import. The type of licence differs based on the possible risk that may be caused in case of failure or malfunction. The importer must be equipped with the facilities necessary for conducting quality inspections and manufacturing and quality control systems. 3. Medical device repair business (Article 16) • A person who intends to engage in the business of repairing medical devices ("repairer") must file a report on the repair business with local governments. The repairer must be equipped with facilities and a quality control system. The manufacturer or importer with a proper licence may conduct repair business without filing a report on the repair business. 4. Distribution business and leasing business (Article 17)

	• A person who intends to engage in the business of distributing medical devices ("distributor") or a person who intends to engage in the business of leasing medical devices ("lessor") must file a report on the distribution business or leasing business with local government having jurisdiction over the place of business. The report must be filed separately for each place of business. The filing of a report on distribution or leasing business is exempted for the following cases: (i) Where a manufacturer or importer of medical devices distributes or leases medical devices manufactured or imported by him/her to a medical device handler; (ii) Where a business that has filed a distribution business report engages in a leasing business; (iii) Where a business that has established a pharmacy or a drug wholesaler distributes or leases medical devices; (iv) Where a business distributes medical devices for the control of conception or medical devices for self-diagnosis to be used at places other than medical institutions. After completing the aforementioned requirements, there are other obligations to comply with under the Medical Device Act. The major obligations include: 1. Approval, certification, or report on modification (Article 12) Where any changes (e.g. a change in location) occur in any information regarding permission or certification already granted or a notification already filed, **a manufacturer, importer, repairer, distributor, or lessor** must obtain approval or certification for modification from or file a report on modification to the Ministry of Food and Drug Safety. 2. System maintenance and reporting obligations (Article 13)

	A manufacturer, importer, or repairer must maintain facilities and manufacturing and quality control systems and must comply with specifics regarding production control, including self-testing as prescribed by the Ordinance of the Prime Minister In addition, a **manufacturer, importer, or repairer** must report to the Ministry of Health and Welfare and the Ministry of Food and Drug Safety on the production, import, or repair status of medical devices. 3. Disclosure of expense reports on details of economic profits provided to relevant persons (Article 13-2) The manufacturer (and the person that conducts marketing of medical devices produced by the manufacturer) and importer must disclose expense reports on details of economic profits provided to medical personnel, persons or entities establishing medical institution, or persons working for medical institutions within three months from the expiry of each fiscal year and must keep the relevant expense report, related books, and evidential materials for five years.
Cybersecurity requirements	
4. Is Medical Device Software subject to general cybersecurity regulations in your jurisdiction? If so, (a) how do these regulations apply to Medical Device Software? (b) Can you provide a brief introduction of the general cybersecurity requirements that are applicable to the Medical Device Software?	The Personal Information Protection Act (**PIPA**) is the principal data protection law that applies to all data controllers that process personal information and stipulates the data controllers' obligations to take security measures. To be specific, the PIPA requires every data controller to take administrative, technical, and physical security measures for the protection of personal information. Such measures include, but are not limited to, the followings: • Administrative measures: — Establish and implement an Internal Data Management Plan; — Limit authority to access personal information. • Technical measures: — Implement an access control system;

		— Encryption for safely storing and transferring personal information; — Preserve and protect log files to monitor access records; — Install security programs and keep them up to date. • Physical measures: — Physically restrict access to sites, offices, and data rooms. Thus, in case a Medical Device Software processes personal information under the PIPA (refer to Section 5 below), the data controller of such Medical Device Software must comply with the security measures stated above. Additionally, depending on whether the Medical Device Software provides service online or whether it uses cloud services, the data controllers thereof shall comply with the aforementioned laws.
5.	In addition to the generally applied cybersecurity requirements, are there any cybersecurity requirements that are specifically set for Medical Device Software, including any cybersecurity related requirements in its development, testing, deployment, and maintenance of Medical Device Software?	In addition to the above laws, there are laws and guidelines for medical records and medical device that stipulate cybersecurity requirements. The major laws and guidelines include: • **The Medical Service Act**, which provides cybersecurity requirements related to the medical records. The act states the requirements (e.g. specification of system) for the Electronic Medical Record (**EMR**) system (Article 23-2) and medical record keeping system (Article 40-3). The Act also regulates a breach of medical treatment information in EMR (Articles 23-3 and 23-4). • **The Standards for facilities and equipment required for the management and preservation of EMR by the Ministry of Health and Welfare** (the **Standards**), which state specific cybersecurity requirements for EMR, including backup, network, location of servers, etc. In case a Medical Device Software is related to EMR, the Standards would apply.

	• **The Guidelines on Cybersecurity Approval and Assessment of Medical Devices issued by the Ministry of Food and Drug Safety** (the **Guidelines**), which stipulate the specific matters related to the approval and assessment under the Medical Device Act, and provide cybersecurity standards specific to medical devices capable of wired/wireless communication or devices equipped with communication networks. These Guidelines state requirements necessary for approval and assessment of medical device software, such as the conformity verification, details of cybersecurity requirements, etc., and also provide the Medical Device Cybersecurity Requirements Checklist.
Data Protection requirements	
6. How is data collected and processed by Medical Device Software regulated in your jurisdiction?	As mentioned above, the PIPA is the main law governing processing and protection of personal information in Korea. Data controllers that collect and process personal information must comply with the following in accordance with the PIPA. 1. Personal information, including sensitive information Under the PIPA, the term "personal information" is defined as the information pertaining to a living person by which it is possible to identify a person (e.g. name, resident registration number, visual image, etc.). The personal information also includes information that, even if by itself cannot identify a particular person, may be easily combined with other information to identify a particular individual and pseudonymised personal information incapable of identifying a particular individual without use or combination of additional information. In particular, personal information related to health is considered "sensitive information" under the PIPA. As it is highly expected that Medical Device Software would collect and process personal information related to health, its data controller would be subject to the requirements related to the sensitive information in

	addition to the general requirements for personal information. 2. Collecting and processing The PIPA provides various legal bases for collection and processing. In general, data controllers collect and process personal information based on consent from data subjects. However, certain information that is essential for the execution and performance of a contract between a data controller and a data subject, complying with laws and regulations, protecting life, protecting physical or economic interests in an urgent situation, protecting a data controller's legitimate interest, etc., may be collected and used without consent. Meanwhile, the PIPA stipulates stricter requirements for sensitive information. This means that the processing of sensitive information is prohibited in principle unless there is separate explicit consent from data subjects or such processing is required or permitted by laws and regulations. Moreover, the provision of personal information to third parties, entrustment of personal information processing, and overseas transfer of personal information would be subject to additional disclosure and/or consent requirements under the PIPA. 3. Other requirements As mentioned in Section 3, data controllers collecting and processing personal information must comply with the security measures under the PIPA. In addition, data controllers should take necessary measures when data subjects exercise their rights stipulated in the PIPA.
7. Is there any data localisation requirement for the data generated or processed via the Medical Device Software?	There are no general data localisation requirements for the generation or processing of data via Medical Device Software. However, in accordance with the Standards for facilities and equipment required for the management and preservation of EMR provided by the Ministry of Health and Welfare, if the

		EMR is managed and stored outside of hospitals, the physical location of the EMR system and its backup equipment shall be within Korea. Thus, if a data generated or processed via the Medical Device Software is related to the EMR, the above Standards would apply.
8.	From a compliance perspective, are the above regulatory requirements being fully implemented in practice? Are there any compliance risks that the Medical Device Software operators may need to note?	Yes, the above regulatory requirements are fully implemented in practice. Failure to comply with the above laws may result in criminal charges, criminal fines, and administrative penalties. Specific risks may differ according to the details of non-compliance.
Miscellaneous		
9.	For summarising purposes, could you please list all the laws / regulations / guidelines and the relevant regulators in your jurisdiction that pertain to medical device cybersecurity?	• Personal Information Protection Act • Act on the Promotion of Information and Communications Network Use and Information Protection • Act on the Development of Cloud Computing and Protection of its Users • Medical Service Act • The Standards for facilities and equipment required for the management and preservation of EMR • Guidelines on Cybersecurity Approval and Assessment of Medical Devices
10.	For medical device cybersecurity, do you know any plans by local regulators to issue any specific rules, guidelines, or standards? What are the areas where regulations are most needed from your perspective?	There are several pieces of legislation or amendments of laws related to the data subject's right to portability of medical data pending at the National Assembly. As the general right to data portability under the PIPA will be effective between March 2024 and March 2025, the medical data specific laws are expected to be passed around the same time. It is also anticipated that other laws and/or regulations related to the medical data may be amended to reflect the changes described above.

Singapore

Latest update: August 2023

Definition and scope	
11. In your jurisdiction, what is the legal definition for medical devices?	The term "medical device" is defined in the First Schedule of the Health Products Act 2007 as: (a) any instrument, apparatus, implement, machine, appliance, implant, reagent for *in vitro* use, software, material or other similar or related article that is intended by its manufacturer to be used, whether alone or in combination, for humans **for one or more of the specific purposes** of - (i) diagnosis, prevention, monitoring, treatment or alleviation of disease; (ii) diagnosis, monitoring, treatment or alleviation of, or compensation for an injury; (iii) investigation, replacement, modification or support of the anatomy or of a physiological process, mainly for medical purposes; (iv) supporting or sustaining life; (v) control of conception; (vi) disinfection of medical devices; or (vii) providing information by means of in vitro examination of specimens derived from the human body, for medical or diagnostic purposes, and which **does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means**, but which may be assisted in its intended function by such means; and (b) the following articles:

	(i) any implant for the modification or fixation of any body part; (ii) any injectable dermal filler or mucous membrane filler; (iii) any instrument, apparatus, implement, machine or appliance intended to be used for the removal or degradation of fat by invasive means.
12. (a) In your jurisdiction, are all types of health care related software (i.e., computer programs, applications, or systems specifically designed to support and enhance various aspects of healthcare delivery and management, including those in independent form and those attached to a physical medical device) regarded as medical devices based on the above definition? (b) If not all the health care related software can be covered by the definition of medical devices, is it clearly defined which kinds of medical related software will be regulated as a medical device and which are not?	(a) Yes, insofar as the intended use serves the above specific purposes. Based on the First Schedule above, it includes software that is **intended to be used**, whether alone or in combination, for the above specific purposes. Under s 2 of the Health Products (Medical Devices) Regulations 2010, "intended use" or "intended purpose" in relation to a medical device or its process or service, means the objective intended use or purpose of the medical device, process or service, as reflected in the specifications, instructions and information provided by the product owner of the medical device. Additionally, the primary mode of action by which the intended purpose is achieved should also be considered. For a medical device, the primary mode of action by which the intended purpose is typically achieved is by physical means (including mechanical action, replacement of, or support of the anatomy or of a physiological process). (b) N.A.
General regulatory requirements	
13. For medical software that is regulated as a medical device ("**Medical Device Software**"), what regulatory steps (e.g., additional clinical trials, approvals, tests, maintenance, supplementary registration after software update) are required to be completed before	Before manufacturing, importing, and supplying medical devices in Singapore, the supplier needs to register the medical device with the Health Science Authority Singapore (**HSA**). Registration requirements are dependent on the medical device's risk classification and the type of evaluation route. Requirements include:

it can be approved for market launch and during the post-marketing period?	(a) Essential Principles for Safety and Performance checklist; (b) Labelling requirements; (c) Software versioning and traceability; (d) Design verification and validation; (e) Clinical evaluation; (f) Risk management; (g) Cybersecurity. Additionally, all medical device dealers must apply for a dealer's licence. Dealers must have a Quality Management System that meets requirements to ensure the safety, quality and performance of medical devices they are dealing in, in accordance with the Good Distribution Practices.
Cybersecurity	
14. Is Medical Device Software subject to general cybersecurity regulations in your jurisdiction? If so, (a) how do these regulations apply to Medical Device Software? (b) Can you provide a brief introduction of the general cybersecurity requirements that are applicable to the Medical Device Software?	The Cybersecurity Act (**CSA**) sets out a framework for monitoring Critical Information Infrastructures (**CIIs**), including imposing obligations on owners of CIIs to report cybersecurity incidents, and provides for the appointment of a Commissioner of Cybersecurity to, among other things, oversee and promote the cybersecurity of computers and computer systems in Singapore. Under the CSA, the Commissioner of Cybersecurity may designate a computer or computer system as a CII under the CSA if the Commissioner is satisfied that (a) the computer or computer system is necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore; and (b) the computer or computer system is located wholly or partly in Singapore. The list of essential services currently includes healthcare, and specifically acute hospital care services and services relating to disease surveillance and response. Medical devices do not specifically fall under these categories. However, it is possible that if certain medical devices grow in importance, they might be designated a CII

	under the CSA. If so, the owner of the CII would have certain obligations, such as: • Reporting cybersecurity incidents to the Commissioner of Cybersecurity; • Conducting regular cybersecurity audits and risk assessments of CII; • Furnishing information on the design, configuration and security of the CII to the Commissioner of Cybersecurity upon written notice to do so.
15. In addition to the generally applied cybersecurity requirements, are there any cybersecurity requirements that are specifically set for Medical Device Software, including any cybersecurity related requirements in its development, testing, deployment, and maintenance of Medical Device Software?	According to regulatory guidelines issued by the HSA for software medical devices, cybersecurity considerations must be considered and manufacturers must devise an effective cybersecurity strategy that addresses all possible cybersecurity risks, not only during development but throughout the useful life of the software medical device.[1] For example, when developing a software medical device, a cybersecurity plan should be devised to include the following considerations, (non-exhaustive): (i) a secure device design; (ii) having proper customer security documentation; (iii) conduct cyber risk management; (iv) conduct verification and validation testing; and, (v) having an on-going plan for surveillance and timely detection of emerging threats. Separately, under the Cybersecurity Labelling Scheme for Medical Devices (**CLS (MD)**), medical devices are rated according to their levels of cybersecurity provisions. **This is a voluntary scheme.** The label aims to improve security awareness by making the cybersecurity provisions of medical devices more transparent to healthcare users and empowers them to make informed purchasing decisions. This scheme only applies to medical devices pursuant to the First Schedule of the Health Products Act (as above) and contains the following characteristics:

[1] https://www.hsa.gov.sg/docs/default-source/hprg-mdb/guidance-documents-for-medical-devices/regulatory-guidelines-for-software-medical-devices---a-life-cycle-approach_r2-(2022-apr)-pub.pdf

	(i) Handles personal identifiable information and clinical data and is able to collect, store, process, or transfer such data; and/or (ii) Connects to other devices, systems, and services and has the ability to communicate using wired and/or wireless communication protocols through a network of connections. The four levels of cybersecurity are as follows:[2] 1. Level 1 – Security baseline requirements: a. Manufacturers need to meet the existing mandatory HSA requirements based on international standards adopted by major medical device regulatory bodies (e.g. US FDA, Health Canada, Japan MHLW, TGA Australia). 2. Level 2 – Enhanced Security Requirements: a. Manufacturers need to meet the enhanced security requirements titrated from MDS2,[3] Post-market policies and existing CLS standards. 3. Level 3 – Software binary analysis, and time bound black-box penetration testing (requires third party independent laboratory testing): a. The software of the medical device (i.e. firmware, mobile applications if available) undergo automated binary analysers to ensure no known critical software weakness, vulnerabilities or malware. b. The device will also undergo time bound black-box[4] penetration testing to provide a basic level of resistance against common cybersecurity attacks. 4. Level 4 – Time Bound White-box Security Evaluation:

[2] https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls(md)/cls(md)-public-industry-consultation-slides.pdf?sfvrsn=8a61cd6c_1

[3] Manufacturer Disclosure Statement for Medical Device Security.

[4] Black-box penetration test: Evaluator performs testing using only limited information (i.e. only user guidance manuals that are provided with the device).

	a. The device undergoes a time bound whitebox[5] security evaluation to provide higher level of resistance against cybersecurity attacks.
Data protection requirements	
6. How is data collected and processed by Medical Device Software regulated in your jurisdiction?	The Personal Data Protection Act 2012 (**PDPA**) provides a baseline standard of protection for personal data in Singapore. It comprises various requirements governing the collection, use, disclosure and care of personal data in Singapore. As health data is potentially more sensitive in nature, tighter security arrangements must be employed to ensure that health data is kept secure. According to the advisory guidelines issued by the Personal Data Protection Commission (**PDPC**) on the healthcare sector,[6] there is no 'one size fits all' solution for organisations to comply with the Protection Obligation under the PDPA. Generally, where the personal data stored is regarded as more confidential and where the adverse impact to individuals is significantly greater if such personal data were inadvertently accessed (e.g. relating to sensitive medical conditions), tighter security arrangements should be employed. Healthcare institutions should consider the nature of the personal data in their possession or under their control (as the case may be) to determine the security arrangements that are reasonable and appropriate in the circumstances.
7. Is there any data localisation requirement for the data generated or processed via the Medical Device Software?	There is no specific data localisation requirement. However, there are general transfer limitation obligations in the PDPA. Specifically, Section 26 of the PDPA limits the ability of an organisation to transfer personal data outside Singapore. In particular, section 26(1) provides that an organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to personal

[5] White-box security evaluation: Evaluator is provided with information on the design/implementation of certain security functionalities (i.e. cryptographic functions). With more information, evaluator would be able to devise targeted tests and better assess the security functionalities of the device.
[6] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Sector-Specific-Advisory/advisoryguidelinesforthehealthcaresector28mar2017.pdf

		data so transferred that is comparable to the protection under the PDPA.
8.	From a compliance perspective, are the above regulatory requirements being fully implemented in practice? Are there any compliance risks that the Medical Device Software operators may need to note?	Yes. Medical Device Software operators should be aware of compliance risks under the PDPA in relation to health data collected by its medical device. It should be noted that the PDPC is empowered to investigate and enforce the PDPA provisions. If found to have breached any provisions, the PDPC can direct the organisation to take steps to ensure compliance such as to: • Stop collecting, using or disclosing personal data in contravention of the PDPA; • Destroy personal data collected in contravention of the PDPA; • Provide access to or correct the personal data; and/or • Pay a financial penalty.
Miscellaneous		
9.	For summarising purposes, could you please list all the laws / regulations / guidelines and the relevant regulators in your jurisdiction that pertain to medical device cybersecurity?	Health Products Act Health Products (Medical Devices) Regulations 2010 Personal Data Protection Act 2012 HSA Regulatory Guidelines for Software Medical Devices 2022 PDPC Advisory Guidelines on Key Concepts in the Personal Data Protection Act PDPC Advisory Guidelines for the Healthcare Sector Cybersecurity Labelling Scheme
10.	For medical device cybersecurity, do you know any plans by local regulators to issue any specific rules, guidelines, or standards? What are the areas where regulations are most needed from your perspective?	The Ministry of Health (MOH), Cyber Security Agency of Singapore (CSA), Health Sciences Authority (**HSA**), and Integrated Health Information Systems (**IHiS**) has issued an Industry Consultation on the Proposed Cybersecurity Labelling Scheme for Medical Devices on 25 January 2023. Given the growing importance of cybersecurity, it may be necessary to make such cybersecurity labelling requirements

	mandatory, especially in the area of medical devices where sensitive healthcare data is being processed.

Thailand

Latest update: July 2023

Definition and scope	
1. In your jurisdiction, what is the legal definition for medical devices?	The definition of a medical device in Thailand is similar to the European Union Medical Device Directive (EU MDD). Section 4 of the Thailand Medical Device Act, defines a "medical device" as: ***Section 4*** *(1) An instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, **software**, material or other similar or related article that the manufacturer or the product owner has an intention for use with either humans or animals, no matter that it is to be used alone or in combination, for one or more of the following specific purposes:* *(a) Diagnosis, prevention, monitoring, treatment or alleviation of disease;* *(b) Diagnosis, monitoring, treatment, alleviation or healing of an injury;* *(c) Investigation, replacement, modification, or support of the anatomy or of a physiological process;* *(d) Sustaining or resuscitation of life;* *(e) Control of conception;* *(f) Supporting or replenishment of disabilities, or disability;* *(g) Providing information following the investigation of body specimens for medical or diagnostic purposes;* *(h) Disinfection or killing germs of medical devices.*

		(2) Accessories for use together with a device according to (1). *(3) Any instrument, apparatus, machine, product, or other materials that the Minister of Public Health announces is a medical device.* *The achievement of intended uses as prescribed above must not be derived from the pharmacological, immunological or metabolism occurring inside human or animal bodies.*
2.	(a) In your jurisdiction, are all types of health care related software (i.e., computer programs, applications, or systems specifically designed to support and enhance various aspects of healthcare delivery and management, including those in independent form and those attached to a physical medical device) can regarded as medical device based on the above definition? (b) If not all the health care related software can be covered by the definition of medical devices, is it clearly defined which kinds of medical related software will be regulated as a medical device and which are not?	Software, either used alone or attached to a physical medical device, is explicitly mentioned in the definition of a medical device. However, the intended use is an essential element for determining whether or not a particular software application is a medical device. According to the ruling criteria of the Thai Food and Drug Administration, software can be classified as a medical device if the following conditions are met: 1) If it is intended for disease diagnosis; 2) If it is intended for disease monitoring; or 3) If it is intended to control or monitor the performance of medical devices (e.g. embedded software intended to control X-ray machines).
General Regulatory Requirements		
3.	For medical software that is regulated as a medical device ("**Medical Device Software**"), what regulatory steps (e.g., additional clinical trials, approvals, tests, maintenance, supplementary registration after software update) are required to be completed before it can be approved for market	The medical device software must be registered with the Thai FDA prior to importation or domestic manufacture for commercial purposes. To register an imported software medical device in Thailand, there are two (2) steps to undertake: *Step 1: Obtaining the Business Place Registration Certificate as a Medical Device Importer* Any party who wishes to import a medical device into Thailand must register their place of business as a medical

	launch and during the post-marketing period?	device importer with the Thai FDA. The eligible party must be a company registered with the Ministry of Commerce of Thailand with a physical address in Thailand. The business establishment registration certificate as a medical device importer remains valid for five (5) years, and must be renewed every five (5) years. The government fee for obtaining the certificate is approximately USD 530. This process takes around 30 business days. *Step 2: Software Medical Device Registration* After obtaining the establishment registration certificate from the Thai FDA, an importer (also known as the marketing authorisation holder) must apply for and obtain a Product Licence or MA Licence for the software intended to be imported for sale in Thailand. As of today, the product licence for the importation of a medical device remains valid for five (5) years, and must be renewed every five (5) years. If the software medical device deploys artificial intelligence (AI) technology, a software validation study and clinical evidence are required for product registration with the Thai FDA. In addition, the AI based application on smart phone must have the measurements on cybersecurity protection and health data protection. Such measurements must be submitted to the Thai FDA during the product registration.
Cybersecurity Requirements		
4.	Is Medical Device Software subject to general cybersecurity regulations in your jurisdiction? If so, (a) how do these regulations apply to Medical Device Software? (b) Can you provide a brief introduction of the general cybersecurity requirements that are applicable to the Medical Device Software?	There is no direct mention of cybersecurity measures in the Medical Device Act. Nonetheless, software as a medical device is prone to cyberattack. Healthcare providers in particular prefer medical devices to be equipped with telemedicine technology and an Application for Programming Interface (API) to be connected with a healthcare facility database. However, connecting the medical device to the internet should be done with caution. Under the Cybersecurity Act, certain healthcare organisations (e.g. healthcare facility, software medical device service provider) must protect, manage, and reduce cyber risks by complying with the National Cyber Security Committee

		(NCSC) Guidelines and adhering to the duties prescribed in the Act. The Medical Council of Thailand also prescribes the Guidelines on Telemedicine and Online Clinic in 2020. According to the Guidelines, the information technology and related devices that collect, store, transmit, exchange and process patient information for telemedicine/online clinics must meet the information security standard and comply with the Electronic Transaction Act 2019 and Personal Data Protection Act 2019. Regarding personal data, Thailand has for many years considered patient data to be private and required its handling to be in keeping with general principles of privacy and consent. Until June 2022, this was regulated by way of the requirements for licensed healthcare professionals under their professional ethical guidelines. In 2019, the Personal Data Protection Act (PDPA) was enacted, and on 1 June 2022, it took full effect. Now the entire understanding of personal data has taken on more relevance. The PDPA divides regulations between general data and sensitive data. Health data is classified as sensitive data requiring a patient's consent before this data can be collected or shared. There are a few exceptions, such as preventing physical harm to the patient and use for non-profit or scientific research purposes.
5.	In addition to the generally applied cybersecurity requirements, are there any cybersecurity requirements that are specifically set for Medical Device Software, including any cybersecurity-related requirements in the development, testing, deployment, and maintenance of Medical Device Software?	Not applicable.
Data Protection Requirements		
6.	How is data collected and processed by Medical Device	The main act regulating data privacy and protection in Thailand is the Personal Data Protection Act B.E. 2562

	Software regulated in your jurisdiction?	(2019) (PDPA). The PDPA came into effect on 1 June 2022 and applies both territorially and extra-territorially. Under the PDPA, personal data is separated into three (3) main categories, including personal data, sensitive data (including health data) and minor data. The personal data processed by Medical Device Software is subject to the regulation under the PDPA. Section 37(1) states that to "provide appropriate security measures for preventing unauthorised or unlawful loss, access, use, alteration, correction or disclosure of Personal Data, such measures must be reviewed when it is necessary, or when the technology has changed in order to efficiently maintain the appropriate level of security and safety. It shall also be in accordance with the minimum standard specified and announced by the Committee." Additionally, the Data Controller shall take action to prevent unlawful disclosures, employ a system for erasure or destruction of the Personal Data when the retention period ends, and notify the authority of any breach of personal data.
7.	Is there any data localisation requirement for the data generated or processed via the Medical Device Software?	Not applicable.
8.	From a compliance perspective, are the above regulatory requirements being fully implemented in practice? Are there any compliance risks that the Medical Device Software operators may need to note?	If a software product processes only unidentified patient data and does not include personal information, the software product is not subject to the PDPA, so long as such information cannot be used directly or indirectly to identify a natural person.
Miscellaneous		
9.	For summarising purposes, could you please list all the laws / regulations / guidelines and the relevant regulators in your jurisdiction that pertain to medical device cybersecurity?	— The Cybersecurity Act B.E. 2562 (2019); — Civil and Commercial Code of Thailand; — Medical Device Act B.E. 2551 (2008), as amended in 2019 (MDA); — Product Liability Act B.E. 2551 (2008) (PLA);

	— Personal Data Protection Act B.E. 2562 (2019) (PDPA); and — Private industry association standards/best practices under the Thai Medical Device Technology Industry Association, if applicable.
10. For medical device cybersecurity, do you know any plans by local regulators to issue specific rules, guidelines, or standards? What are the areas where regulations are most needed from your perspective?	The Thai FDA has drafted the Guideline on Regulation of Software and A.I. Software as a Medical Device (SaMD). The Thai FDA has reviewed and referred the Guidelines of other benchmark jurisdictions including: — Regulatory Guidelines for Software Medical Device - A Life Cycle Approach; — Japan Guidance for Evaluation of Artificial Intelligence - assisted Medical Imaging Systems for Clinical Diagnosis; and — MDCG 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 - Medical Device Regulation (MDR) and Regulation (EU) 2017/746—IVDR The Guidelines of the Thai FDA shall include the cybersecurity risk analysis and corrective action plan/ measurements for prevention the cyber-attack. In addition, the SaMD which connects to the internet must have the personal data protection measurement complying with the Personal Data Protection Act 2019. It is contemplated that the Thai Guidelines will be implemented in next year.

Vietnam

Latest update: September 2023

Definition and scope		
1.	In your jurisdiction, what is the legal definition for medical devices?	According to Clause 1, Article 2 of Decree 98/2021/ND-CP, medical device means: any instrument, implant, apparatus, material, in vitro reagent or calibrator, or software that meets the following requirements: — It is intended, by the product owner to be used, whether alone or in combination, for human beings for the purpose of one or more of the following: • Diagnosis, prevention, monitoring, treatment or alleviation of disease, or compensation for an injury or trauma; • Investigation, replacement, modification or support of the anatomy or of a physiological process; • Supporting or sustaining life; • Control of conception; • Disinfection of medical devices; • Providing information serving diagnosis, monitoring or treatment through examination of specimens derived from the human body. — The device does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but may be assisted in its function by such means to serve the purposes mentioned above.
2.	(a) In your jurisdiction, are all types of healthcare-related software (i.e. computer programmes, applications, or systems specifically	Software, either used alone or attached to a physical medical device, is explicitly mentioned in the definition of a medical device mentioned in Decree 98/2021/ND-CP. Other than this, there is no further specific guidance on software medical

	designed to support and enhance various aspects of healthcare delivery and management, including those in independent form and those attached to a physical medical device) regarded as medical device-based on the above definition? (b) If not all healthcare-related software are covered by the definition of medical devices, is it clearly defined which kinds of medical-related software will be regulated as a medical device and which are not?	device. Therefore, in Vietnam, healthcare-related software will be regulated as a medical device if it meets the above requirements for a medical device.
General Regulatory Requirements		
3.	For medical software regulated as a medical device ("Medical Device Software"), what regulatory steps (e.g. additional clinical trials, approvals, tests, maintenance, supplementary registration after software update) must be completed before it can be approved for market launch and during the post-marketing period?	Medical Device Software must be registered with the authority assigned by Vietnam Ministry of Health (MOH) prior to importation or its domestic launch for commercial purposes. To register an imported software medical device in Vietnam, the first step is to determine the correct classification of your medical device. Vietnam's medical device classification system is composed of four classes of increasing risk: Class A (low risk) Class B (low-medium risk) Class C (medium-high risk) Class D (high risk) Based on the classification, the following regulatory pathways exist: — Applicants of all Class A and B medical devices must submit a Declaration of Applied Standards application to the local/regional Department of Health where the applicant is established. — Applicants of Class C and D devices must submit a Marketing Authorisation Registration application to the

	Department of Medical Equipment and Construction (DMEC) under the MOH for review and approval. So far, the regulations are silent on any additional requirements for software medical devices in Vietnam.
Cybersecurity Requirements	
4. Is Medical Device Software subject to general cybersecurity regulations in your jurisdiction? If so, (a) how do these regulations apply to Medical Device Software? (b) Can you provide a brief introduction of the general cybersecurity requirements that are applicable to the Medical Device Software?	There is no direct mention of cybersecurity measures in the specific regulations on medical devices. Nevertheless, software as a medical device is prone to cyberattack. The Vietnamese government has acted swiftly to adopt Industry 4.0, extending this to the digitisation of healthcare. The government is encouraging investors to participate in the development of digital health. Accordingly, healthcare providers now prefer a medical device to be equipped with telemedicine technology and an Application for Programming Interface (API) that can be connected with a healthcare facility database. However, caution should be exercised when connecting a medical device to the internet. Medical Device Software is subject to the broad regulatory framework on Cybersecurity (e.g. Law on Network Information Security; Law on Cybersecurity and Personal Data Protection Decree). Accordingly, the following acts are strictly prohibited in the network environment of Medical Device Software: • Distorting history, denying revolutionary achievements, undermining the great national unity bloc, insulting religion, discrimination based on gender or race; • Disseminating false information that causes confusion among the people, causes damage to socio-economic activities, causes difficulties for the operation of state agencies or those that perform official duties, infringes upon the legitimate rights and interests of the people, or the laws of other agencies, organisations and individuals; • Engaging in prostitution, social evils, or human trafficking; the posting of lewd, depraved, or criminal information; undermining the nation's fine customs and

	traditions, social morality or the health of the community; • Instigating, enticing, or inciting others to commit crimes. If a medical device connects to a network, the network operator must apply the measures to protect network security including the following: • Network security assessment; • Assessment of network security conditions; • Checking network security; • Monitoring network security; • Responding to and resolving network security incidents; • Fighting to protect network security; • Using cryptography to protect network information; • Preventing or requesting the suspension of the supply of network information; prohibiting or temporarily suspending the activities of setting up, providing and using telecommunications networks or the internet as well as forbidding the manufacture and use of radio transmitters and receivers in accordance with the law; • Requesting deletion or granting access to delete illegal information or false information on cyberspace that infringes upon national security, social order and safety, and the lawful rights and interests of agencies, organisations and individuals; • Collecting electronic data related to activities that infringe upon national security, social order and safety, and the legitimate rights and interests of agencies, organisations and individuals on cyberspace; • Blocking or restricting the operation of information systems; temporarily suspending or requesting the halt in operations of the information system or revoking domain names in accordance with the law; • Prosecuting, investigating, and adjudicating according to the provisions of the Criminal Procedure Code.

5.	In addition to the generally applied cybersecurity requirements, are there any cybersecurity requirements that are specifically set for Medical Device Software, including any cybersecurity-related requirements in the development, testing, deployment, and maintenance of Medical Device Software?	Additionally, Medical Device Software is subject to specific regulatory legislation in the medical sector (e.g. Circular on telemedicine, Circular on online healthcare services, etc.). Among requirements applicable to the telemedicine platform in Vietnam, the application's software security must adhere to the following requirements for information security assurance: a) There must be regulations on error logging and the error-handling process, especially errors in assurance of security in checking and testing application software; b) Software versions, including the source programme that needs to be managed in a centralised manner, must be stored and secured. There must be regulations on granting privileges to each user to manipulate files; c) A periodic plan for source code verification must be formulated to prevent malicious codes and vulnerabilities; d) The application software vendor must undertake that its product contains no malicious code.
Data Protection Requirements		
6.	How is data collected and processed by Medical Device Software regulated in your jurisdiction?	After a protracted period of deliberation, the Vietnamese government ultimately passed the country's "historic," first-ever Personal Data Protection Decree (PDPD) on 17 April 2023, as Decree No. 13/2023/ND-CP. The PDPD is a landmark legal instrument that integrates all of Vietnam's disparate data protection legislation with the potential to bring them closer to the EU's General Data Protection Regulation (GDPR) requirements. According to PDPD, personal data is split into two different categories - basic personal data and sensitive personal data. Basic personal data includes name, date of birth, gender, nationality, personal photos, phone number, identification number, marriage status, history of one's cyberspace activities, and so on. Sensitive personal data is more private and, if violated, will jeopardise a person's legitimate rights and interests. Accordingly, sensitive personal data includes, among other things, political and religious views, health

	status and private-life information as recorded in medical records, racial or ethnic origins, sexual orientation, criminal records, customer information of credit institutions/foreign bank branches/payment intermediary service providers, or location data. The personal data collected and processed by Medical Device Software is subject to the PDPD's requirements on personal data protection. Where the type of data collected or processed falls under the categories of sensitive personal data, the operator of the Medical Device Software is also required to comply with the more stringent requirements for protection of sensitive personal data. The processing of personal data includes these eight basic tenets: (i) the processing is in accordance with the law (lawfulness); (ii) data subjects must be informed of every activity involving the processing (transparency); (iii) personal data shall be processed only for the purposes registered and announced in relation to the processing (purpose limitation); (iv) personal data collected must be relevant and confined to the extent and purposes of the processing (data minimisation); (v) personal data must be updated and supplemented in accordance with the processing's purposes (accuracy); (vi) personal data must be subject to protection and security measures during the processing (integrity, confidentiality and security); (vii) personal data shall be kept only for a term appropriate with the processing's purposes (storage limitation); and (viii) the Controller and Controller-Processor must comply with the above principles and demonstrate their compliance (accountability). The standards for processing sensitive personal data appear to be a bit stricter than those for basic personal data. More specifically, the protection of sensitive personal data would necessitate (i) all of the managerial and technical measures required for the protection of basic personal data; (ii) the

		appointment of a Data Protection Officer (DPO) and/or an internal personal data protection department (DPD) (information on the DPD and/or the DPO should be notified to the authority); and (iii) notification to data subjects that their sensitive personal data is processed except in specified cases. It is required that (i) when obtaining consent from the data subject, the data subjects must be informed that the data to be processed is sensitive personal data; and (ii) the data subjects must be notified that their sensitive personal data will be processed. However, it is unclear how these two requirements are different and how they should be combined. Notwithstanding, there are specific provisions in Decision No. 4054/QD-BYT concerning data privacy, which Medical Device Software must comply with, including, but not be limited to, the following: — Application software systems and databases must have a mechanism to backup data, and data must be stored in a safe place and regularly checked in the event of emergency network information security incidents; — Database management system software must be set up to automatically update security patches from the manufacturer; — Images or stored data obtained in the process of remote medical examinations and treatment consultations shall not be used for commercial purposes or any other purposes; — The relevant parties will take responsibility before the law for the disclosure of personal information and health information of patients participating in remote medical consultations.
7.	Is there any data localisation requirement for the data generated or processed via the Medical Device Software?	In Vietnam, the following data must be stored: — Personal data of users in Vietnam; — Data generated by users in Vietnam; — Data on the relationship of service users in Vietnam. Regarding the Cross-Border Transfer of Personal Data generated or processed via Medical Device Software, the

		transferor of personal data must first create a Dossier of Impact Assessment for the Cross-Border Transfer of Personal Data (TIA Dossier) before transferring personal data out of Vietnam. The TIA Dossier must include: (i) information and contact details of the transferor and receiver; (ii) full name and contact details of the organisation and/or individual in charge of the transferor; (iii) description and explanation of the objectives of the personal data processing following the transfer; (iv) description and clarification on the type of personal data to be transferred; (v) description and explanation on compliance with the regulations under the PDPD, detailing the applied measures for personal data protection; (vi) assessment on the impact of the processing, as well as the potential and unwanted consequences and/or damages, and measures to minimise or eliminate such consequences and/or damages; (vii) consent from the data subject; and (viii) documents pertaining to the binding responsibilities of personal data processing between the transferor and transferee.
8.	From a compliance perspective, are the above regulatory requirements being fully implemented in practice? Are there any compliance risks that Medical Device Software operators should note?	After the PDPD came into force in July 2023, Vietnam's entities strictly followed personal data protection measures.
Miscellaneous		
9.	For summarising purposes, could you please list all the laws / regulations / guidelines and the relevant regulators in your jurisdiction that pertain to medical-device cybersecurity?	— Law on Information Technology No. 67/2006/QH11 adopted by the National Assembly of Vietnam on 29 June 2006; — Law on Network Information Security No. 86/2015/QH13 adopted by the National Assembly of Vietnam on 19 November 2015; — Law on Cybersecurity No. 24/2018/QH14 adopted by the National Assembly of Vietnam on 12 June 2018; — Decree No. 13/2023/ND-CP promulgated by the Government on 17 April 2023 on Protection of personal data;

		— Circular No. 53/2014/TT-BYT of the MOH dated 29 December 2014 on provision of online healthcare services; — Circular No. 49/2017/TT-BYT of the MOH dated 28 December 2017 on Telemedicine (“Circular 49”); — Circular No. 46/2018/TT-BYT of the MOH dated 28 December 2018 on electronic medical records; — Decision No. 2628/QD-BYT of the MOH dated 22 June 2020 on approving scheme for remote medical examination and treatment for 2020-2025; — Decision No. 4054/QD-BYT of the MOH dated 22 September 2020 on promulgating interim guidelines and regulations for the organisation of remote medical examinations, treatment consultations and advisories; — Decision No. 5237/QĐ-BYT of the MOH dated 16 December 2020 on the issuance of the list of services temporarily applicable in Telemedicine; — Decision No. 4152/QĐ-BYT of the MOH dated 28 August 2021 on the issuance of temporary guidelines for "Telemedicine for severe COVID-19 patients between treatment facilities"; and — Official Letter No. 2416/BYT-CNTT of the MOH dated 30 April 2020 on the implementation of remote medical examination and treatment consultation activities.
10.	For medical device cybersecurity, do you know of any plans by local regulators to issue any specific rules, guidelines, or standards? In what areas are regulations most needed from your perspective?	So far, there has been no decision by the local regulator to issue specific rules for software medical devices in Vietnam.

Contact us

Australia

Eugenia Kolivos
Partner
Corrs Chambers Westgarth
T +61 2 9210 6316
E eugenia.kolivos@corrs.com.au

China

Nick Beckett
Managing Partner, CMS Beijing and Hong Kong Offices
Global Co-Head CMS Life Sciences& Healthcare Sector Group
T +86 10 8527 0287/+852 2533 7818
E nick.beckett@cms-cmno.com

India

Sameer Sah
Partner
Khaitan & Co
T +91 22 6636 5000
E sameer.sah@khaitanco.com

Indonesia

Mita Kartohadiprodjo
Partner
Assegaf Hamzah & Partners
T +62 21 2555 9972
E mita.kartohadiprodjo@ahp.id

Japan

Chie Kasahara
Senior Partner
Atsumi & Sakai
T +81 3-5501-2438
E chie.kasahara@aplaw.jp

Korea

Ki Young Kim
Partner
Yulchon LLC
T +82 2 528 5222
E kykim@yulchon.com

Singapore

Lau Kok Keng
Head, Intellectual Property, Sports and Gaming
Rajah & Tann Singapore
T +65 6232 0765
E kok.keng.lau@rajahtann.com

Thailand

Alan Adcock
Partner
Tilleke & Gibbins
T +66 2056 5871
E alan.a@tilleke.com

Vietnam

Thomas J. Treutler
Partner
Tilleke & Gibbins
T +84 28 3936 2068
E thomas.t@tilleke.com

The collaboration presented in this publication is limited to Lifesciences. The information held in this publication is for general purposes and guidance only and does not purport to constitute legal or professional advice.

Assegaf Hamzah & Partners, Atsumi & Sakai, Chen & Lin, CMS, Corrs Chambers Westgarth, Rajah & Tann Singapore LLP, Tilleke & Gibbins and Yulchon LLC are all independent law firms.

Further information about each firm can be found respectively at www.ahp.co.id, www.aplaw.jp/en/, www.chenandlin.com, cms.law, www.corrs.com.au, www.rajahtann.com, www.tilleke.com, www.yulchon.com