RF Quarterly

Volume 3 • Number 2

Emerging medical device cybersecurity regulations in China, Japan, and Singapore

Harshita Menon, MS

Ankita Joshi, MS, MBA

The innovation of medical devices and their interconnectivity with healthcare systems and the internet has raised concerns over patient safety, data security, and the potential for cyberattacks. To address these issues, global regulatory bodies are implementing cybersecurity regulations. Cybersecurity regulations in the US and EU are still evolving, but they are comprehensive and cover a range of issues related to medical device cybersecurity. Medical device cybersecurity regulations are emerging in China, Japan, and Singapore and cover only limited requirements. This article presents key aspects of emerging medical device cybersecurity regulations in China, Japan, and Singapore.

Keywords – China, cybersecurity, Japan, medical device, Singapore

Introduction

There are numerous clinical and interventional benefits associated with the increased availability of digital and interconnected medical devices, but this innovation also brings the potential for cyberattacks and exposes the healthcare systems and patient data to various vulnerabilities. A good example would be the recent Log4j vulnerability, which affected the widely used Apache Log4j logging library that is used globally by numerous healthcare systems to manage logs and diagnose issues.[1] The cybersecurity vulnerability enabled attackers to run the arbitrary code on vulnerable systems, which led to data breaches and numerous security incidents.[1] Such instances have prompted governments worldwide to implement strict regulations to ensure secure and private healthcare systems.[2]

This article will focus on the emerging medical device cybersecurity regulations in China, Japan, and Singapore. Since the countries have unique approaches to cybersecurity, reflecting their different political and economic contexts, we can gain insights into the various challenges and opportunities of addressing cybersecurity in the medical device sector.

The National Medical Products Administration (NMPA) in China, has implemented frameworks for medical device cybersecurity that requires manufacturers to execute security measures throughout the product life cycle. These guidelines also require manufacturers to conduct security risk assessments and provide regular security updates for their medical products.[3] The 2017 Cybersecurity Law of the People's Republic of China requires companies to report cybersecurity incidents and cooperate with government investigations.[4]

In Japan, along with the Personal Informa-

tion Protection Act being revised in 2020 to strengthen protections for personal information, the Pharmaceutical and Medical Device Agency (PMDA) issued guidelines for medical device manufacturers to execute security measures that cover the entire product lifecycle, from design to disposal.[5] The guidelines also require manufacturers to conduct risk assessments, maintain records of security incidents, and provide regular security updates.[5]

In recent years, the Health Science Authority (HSA) in Singapore, like China and Japan, introduced guidelines for medical device cybersecurity, that require manufacturers to monitor and implement measures throughout the product lifecycle by conducting security risk assessments, report any incidents and provide regular security updates to the HAS.[6] As the use of medical devices continues to increase, it is essential to ensure their safety and security and the emerging regulations in the three countries are significant steps toward achieving this goal.

Cybersecurity regulations

China

China has established a comprehensive regulatory framework to address cybersecurity concerns in various industries, including medical devices. The regulatory environment for medical devices in China is governed by the NMPA and the Cybersecurity Administration of China (CAC).[7] The NMPA is responsible for regulating the safety, efficacy, and quality of medical devices, while the CAC oversees the implementation of cybersecurity measures across all industries.[7]

One of the key cybersecurity regulations in China is the Cybersecurity Law 2.0, which was introduced in 2020.[8] The law provides a framework for protecting data privacy, network security, and critical information infrastructure. It requires companies to conduct cybersecurity risk assessments, implement preventive measures, and report any data breaches to the authorities.[7]

In addition to the Cybersecurity Law, the NMPA has issued several guidelines and standards for cybersecurity in medical devices.[8] One of the most significant guidelines is the Technical Guidelines for Cybersecurity of Medical Devices, which outlines the minimum cybersecurity requirements for medical devices.[8] These requirements include encryption, access control, and incident reporting.

However, there are several challenges and limitations with the current regulatory framework for cybersecurity in medical devices in China.[9] One of the key challenges is the lack of clarity and consistency in regulatory requirements, particularly for international manufacturers.[9] The NMPA's regulatory process can be complex and time-consuming, with lengthy product registration timelines.

Another challenge is the lack of standardization and interoperability between different medical devices. The complexity of medical devices and their interconnectedness with other devices and networks can make it difficult to identify and mitigate cybersecurity risks.[9]

China's Cybersecurity Law 2.0 requires companies to conduct cybersecurity risk assessments, implement preventive measures, and report any data breaches to the authorities.

Moreover, there is a need for more collaboration and information sharing between regulators and industry stakeholders. The lack of transparent communication can create uncertainty and hinder the development and implementation of effective cybersecurity measures.

To address these challenges, there are ongoing efforts to improve the regulatory framework for cybersecurity in medical devices in China. For example, the NMPA has introduced a fast-track approval process for innovative medical devices, which could help to reduce the time and costs associated with regulatory compliance.[10] In addition, the government is working to establish a more

standardized approach to cybersecurity risk assessments and certification processes.

Japan

Japan is known for having one of the most advanced and rigorous regulatory environments for medical devices. With the increasing risk of cybersecurity threats to medical devices, the Ministry of Health, Labor and Welfare (MHLW) has taken steps to update and strengthen its regulatory framework to ensure patient safety.

One key development in Japan's cybersecurity regulations for medical devices is the issuance of a new guidebook by the MHLW based on cybersecurity guidelines and recommendations from the International Medical Device Regulators Forum (IMDRF).[11] The new guidebook provides updated coverage of technical requirements including international resistance standards to address cyberattacks and vulnerabilities.

> *One key development in Japan's cybersecurity regulations for medical devices is the issuance of a new guidebook by the MHLW based on IMDRF recommendations.*

Moreover, the PMDA issued a notice in March 2022 for strengthening cybersecurity measures related to medical devices, which includes measures to reduce risk, early detection of incidents, and appropriate response and recovery when an incident occurs.[12] The notice outlines the importance of regularly checking access privileges, implementing multi factor authentication, understanding the status of information assets, and promptly applying security patches.

Japan's regulatory framework for medical devices faces challenges and limitations in terms of cybersecurity due to the lack of clear guidelines on how to assess the cybersecurity of medical devices and the limited resources available to both the regulatory authorities and the medical device manufacturers to address cybersecurity concerns.[13] Furthermore, the regulatory framework may not be keeping up with the rapid pace of technological advancement, leading to new cyber threats that leave devices vulnerable.[13] The reporting of cybersecurity incidents and vulnerabilities due to lack of transparent makes it difficult to identify and address potential risks.[14] Consequently, there are concerns regarding the effectiveness of the current regulatory framework, particularly with the increasing number of cyberattacks targeting medical devices worldwide, which puts patient safety and privacy at risk.[14]

Collaboration among regulatory authorities, manufacturers, and cybersecurity experts is essential to ensure that medical devices remain safe and secure for patients. Japan has taken a proactive approach in ensuring safety of connected medical devices by implementing IMDRF's regulatory framework, which uses a total product lifecycle (TPLC) approach ensuring vulnerability assessment.[15]

Singapore

Singapore's regulatory environment for medical device cybersecurity has undergone significant evolution over the years. In response to the increasing use of connected medical devices and the potential risks of cyberattacks, the HSA has implemented regulations and published supporting guidance to improve the safety of medical devices.

Singapore's Ministry of Health and HSA, the Cyber Security Agency of Singapore (CSA), and Integrated Health Information Systems, a health information agency operating within Singapore, collaborated to develop and roll out the Cybersecurity Labeling Scheme for Medical Devices in 2022.[16] The scheme applies to medical devices that handle sensitive data or can connect to other devices, systems, and services. The primary goal of the labeling scheme is to allow healthcare providers and consumers to assess how secure medical devices are against cyber risks and make informed purchasing decisions.[17] The new scheme aims to identify

more medical devices with better in-built cybersecurity and incentivize manufacturers to develop more secure medical devices.[17] However, manufacturers may need to pass independent third-party tests to achieve higher levels of certification which could impact the cost and timeline for commercialization of the medical devices.[18]

In addition, in 2022, the HSA also introduced regulatory guidance for software medical devices.[19] The document highlights three classes of software medical devices based on their risk classification, with Class I being the lowest risk and IIb being the highest.

The guidance provides five elements for an appropriate cybersecurity plan, including secure device design, cyber risk management, and an ongoing plan for surveillance and timely detection of emerging threats. It recommends that medical device manufacturers should consider cybersecurity from the very beginning of the development process and take measures to prevent, detect, respond, and recover from foreseeable cyber risks. The document covers various aspects of the lifecycle of software medical devices, including design and development, validation and verification, manufacturing, installation, and maintenance.[19]

One of the major challenges in medical device cybersecurity is the vulnerability of network-connected medical devices to hacking and cyberattacks.[17] These devices, such as insulin pumps, pacemakers, and other implantable medical devices, can be hacked and controlled by unauthorized individuals, leading to potentially life-threatening situations for patients.[17]

To address this, the HSA has implemented regulations requiring medical device manufacturers to submit a cybersecurity risk assessment for all medical devices seeking regulatory approval in Singapore. This risk assessment must include an evaluation of potential cyber threats and vulnerabilities, as well as a plan for managing and mitigating these risks.

The tables on pages 61-62 show the similarities and differences between regulations for China, Japan, Singapore, and the IMDRF (**Table 1**) and those in the US and EU (**Table 2**), and include an evaluation of their effectiveness and potential areas for improvement.

IMDRF and global regulation

The IMDRF is a global regulatory body that plays a significant role in shaping the cybersecurity regulations of medical devices in emerging countries. The forum facilitates international cooperation and information sharing among regulatory authorities to promote harmonized efforts in defining a foundational framework for manufacturers to follow.[20]

The IMDRF's influence on emerging countries' cybersecurity regulations is significant. As many of these countries look to develop their own regulatory frameworks for medical devices, they often turn to IMDRF for guidance and support. The forum also offers developing nations a regulatory model, which is accepted and developed by leading regulatory authorities across the globe.[21]

In 2018, the Global Diagnostic Imaging, Healthcare IT & Radiation Therapy Trade Association (DITTA) proposed a new work item at the IMDRF management committee hearing.[22] The DITTA published a white paper on cybersecurity that outlines seven principles for best cybersecurity practices in medical technology manufacturing.[23] The paper aims to increase manufacturers' cybersecurity sophistication by providing recommendations for identifying threats and incorporating relevant consensus standards. The focus on global harmonization of medical device cybersecurity reflects the need for a reimagined approach as devices become increasingly connected, posing potential threats to patient safety.[24]

In 2019, the cybersecurity working group released its first guidance document on medical device cybersecurity. It was finalized in 2020.[25] The guidance includes premarket and postmarket cybersecurity considerations, covering risk management, security testing, and regulatory submission requirements. The postmarket approach includes vulnerability remediation, incident response, and legacy devices.

Table 1. Comparison of cybersecurity requirements for China, Japan, Singapore, and the IMDRF

Country/organization Point of comparison			
China	**Japan**	**Singapore**	**IMDRF**
Classes for software in/as a medical device			
No software-specific classification for medical devices. SaMD are covered under the NMPA classification of medical devices.[28]	Class I (extremely low risk) applies to non-medical use and excluded from medical devices SaMD risk is classified as: Class II (low), Class III (medium), Class IV (high).[17a]	Software-embedded medical devices are classified based on the 16 risk classification rules for general medical devices and assigned as Class A (nonsterile or sterile), B, C, or D. [29,b]	Categories I, II, III, IV, based on levels of impact on patients or public health (Category I, low risk; Category IV, high risk).[31,c]
TPLC approach to risk management			
Emphasis on risk-based approach to managing TPLC, which includes identifying, evaluating, and mitigating risks throughout product lifecycle.[3]	PMDA implemented IMDRF guidance that uses a TPLC approach for risk management.[12]	Risk management for medical device software follows a systematic approach that includes hazard identification, risk assessment, mitigation implementation, and effectiveness evaluation throughout product lifecycle.[29]	Guiding principles cover TPLC approach for risk management, requiring evaluation and mitigation of cybersecurity risks throughout the TPLC phases such as design, manufacturing, testing, and postmarket monitoring activities.[31]
Access controls			
Medical device cybersecurity regulations require access control measures to be implemented, including authentication authorization, and audit trails, to ensure security of medical devices.[8]	PMDA implemented IMDRF guidance that issues requirements on implementing user access controls.[12]	An appropriate system for version controls and access rights controls should be in place to allow timely tracing of the software.[19]	User access controls must be implemented. including authentication and authorization measures such as passwords, hardware keys, biometrics, or unique signals of intent. Credentials should not be shared across devices or customers.[31]
Incident management			
Manufacturers must establish an incident response plan to identify and respond to cyber-security incidents affecting medical devices.[8]	PMDA implemented IMDRF guidance on requirements for incident response management.[12]	Postmarket plan requirements include a plan for addressing cybersecurity vulnerabilities and a recovery plan for after a cybersecurity incident.[29]	Manufacturers should establish and implement an incident response management policy and team a assess, respond to, and learn from product-related cybersecurity incidents.[31]

continued on page 6

Table 1 (cont.). Comparison of cybersecurity requirements for China, Japan, Singapore, and the IMDRF

Country/organization Point of comparison			
China	**Japan**	**Singapore**	**IMDRF**
Vulnerability assessment			
Manufacturers must perform regular vulnerability assessments and take corrective action to address identified vulnerabilities to ensure medical device security.[8]	PMDA implemented IMDRF guidance requiring vulnerability assessments and analysis to mitigate cybersecurity risk.[12]	Manufacturers must have a formalized process for vulnerability disclosure that involves gathering information, developing mitigation strategies, and disclosing vulnerabilities and approaches to stakeholders.[31]	Requires vulnerability analysis on the target incident and vulnerability assessment as well as a collaborative approach across stakeholders to manage vulnerabilities to mitigate risk to patients and users.[31]
Labeling			
Medical devices must be labeled with information on cybersecurity risks and necessary precautions and contact information for reporting cyber-security incidents.[8]	No specific cybersecurity related labeling requirements.	Under CLSMD, medical devices are rated on their levels of cybersecurity provisions (Levels 1, 2, 3 4), where 1 meets the baseline regulatory cybersecurity requirements, and 2-4 level products must meet enhanced cybersecurity requirements and pass independent third party tests.[29]	No specific cybersecurity-related labeling requirements.
Postmarket			
Manufacturers must have a postmarket surveillance mechanism to monitor cybersecurity risk and incidents and take corrective action if needed.[8]	China uses IMDRF's approach to postmarket surveillance for medical device cybersecurity.[12]	Companies distributing software medical devices must comply with post-market duties, including reporting device defects or malfunctions recalls, safety actions, and device-associated injuries or deaths associated with device use.[29]	The postmarket approach for medical devices includes device operation, information sharing, vulnerability disclosure and remediation, incident response, and legacy devices.[31]

CLSMD, cybersecurity labeling scheme for medical devices; **IMDRF**, International Medical Device Regulatory Forum; **NMPA**, National Medical Products Administration [China]; **PMDA**, Pharmaceutical and Medical Device Agency [Japan]; **SaMD**, software as a medical device; TPLC, total product lifecycle.

[a]Risk class is determined by the degree of contribution the SaMD makes in clinical decision making.[17]
[b]A standalone software (or SaMD) risk classification is classified into the same classes general medical devices and is determined based on state of the patient's health situation or condition: critical, serious, or non-serious; and significance of information provided by SaMD to make healthcare decision such as to treat or diagnose, to drive clinical management, or to inform clinical management.[30]
[c]Risk classification is determined based on state of the patient's health situation or condition: critical, serious, or non-serious; and significance of information provided by SaMD to make healthcare decision such as to treat or diagnose, to drive clinical management, or to inform clinical management.[31]

Table 2. Cybersecurity requirements for US and EU

Country/alliance *Point of comparison*	
US	**EU**
Classes for software in/as a medical device	
Recommends inclusion of device's LoC in the premarket submission. Estimate of severity of injury that maybe caused by the software is designated as Major, Moderate, or Minor. FDA uses IMDRF's approach for categorizing SaMD risk.[32,33,a]	No software-specific or cybersecurity risk-based classification or categories for medical devices.
TPLC approach to risk management	
2022 draft guidance aims to implement security throughout the TPLC.[34,35]	GSPR requirements under the EU MDR require risk management across device lifecycle.[35]
Access controls	
FDA draft guidance recommends device manufacturers' design processes include design inputs for cybersecurity controls.[35]	GSPR requirements under the EU MDR require protection against unauthorized access.[35]
Incident management	
Manufacturers should continuously monitor, identify, and address cybersecurity vulnerabilities in their medical devices during the postmarket phase. FDA provides a risk-based framework for determining when changes cybersecurity-related vulnerabilities require reporting and outlines when reporting requirements may not be enforced.[34,35]	The guidance MDCG 2019-16 covers incident response under the PMS and vigilance requirements.[36]
Vulnerability assessment	
Manufacturers should establish a plan for identifying and communicating with users about vulnerabilities after the device has been released.[35]	MDCG 2019-16 guidance includes vulnerability remediation policy requirements under the PMS and vigilance requirements.[36]
Labeling	
FDA has noted the significance of labeling in managing cybersecurity risk. Updated guidance says any risks transferred to users must be included in the labeling to ensure users can take appropriate actions to manage those risks.[35]	No specific cybersecurity labeling requirements. The guidance only recommends adding information on the device label to identify devices handling sensitive information as a part of IT security policy.[36]
Postmarket	
Manufacturers should continuously monitor, identify, and address cybersecurity vulnerabilities and exploits in their medical devices during the postmarket phase.[37]	Manufacturers must implement postmarket activities for medical devices because cybersecurity vulnerabilities may change.[36]

EU MDR, EU Medical Device Regulation; FDA, Food and Drug Administration [US]; **GSPR,** general safety and performance requirements; **LoC**, level of concern; **MDCG**, Medical Device Coordination Group; **PMS**, postmarket surveillance; **TPLC**, total product lifecycle.

[a]This is not a part of device classification, hazard, or risk analysis.

In 2023, IMDRF released two new cybersecurity guidance – the software bill of materials (SBOM) guidance and legacy devices cybersecurity guidance.[26,27] The SBOM guidance describes what an SBOM is and includes best practices for medical device manufacturers when developing products.[27] The legacy devices cybersecurity guidance focuses on how to apply a TPLC approach to legacy devices. The guidance discusses how stakeholders can identify potential legacy devices and different ways to address their cybersecurity shortcomings.[26]

Cybersecurity framework

All three countries follow a common framework for medical device cybersecurity regulations. The framework is broadly based on the following key principles:

Risk assessment – Manufacturers must conduct risk assessments to identify potential cybersecurity risks and vulnerabilities.

Security controls – Manufacturers must implement appropriate security controls to mitigate cybersecurity risks.

Incident response – Manufacturers must have procedures in place to detect, respond to, and report cybersecurity incidents.

Continuous monitoring – Manufacturers must continuously monitor the security of their devices and take action to address any new threats or vulnerabilities.

Table 3 provides a starting point for visualizing the key components of a cybersecurity framework for medical devices. It shows a general overview of the cybersecurity framework for medical devices in China, Japan, and Singapore, although the specific details may differ among the regulations.

Future developments and implications

Medical device cybersecurity is a rapidly evolving field, and regulatory bodies in China, Japan, and Singapore are likely to continue to update their guidelines and regulations to keep pace with new threats and technologies. For example, the NMPA in China has indicated that it plans to update its guidelines on medical device cybersecurity to reflect the latest international standards and best practices.[38]

In addition, there is increasing recognition of the need for global coordination and harmonization of medical device cybersecurity regulations.[38] The IMDRF, which includes regulatory authorities from around the world, has published guidelines on medical device cybersecurity that are intended to provide a common framework for regulators and manufacturers.[38]

Table 3. Cybersecurity framework for China, Japan, and Singapore

	Country		
Component	China	Japan	Singapore
Regulatory agency	NPMA	PMDA	HSA
Standard followed	ISO/IEC 27001[38]		
Risk assessment	Yes	Yes	Yes
Security controls	Yes	Yes	Yes
Incident response	Yes	Yes	Yes
Continuous monitoring	Yes	Yes	Yes

IEC, International Electrotechnical Commission; **ISO**, International Organization for Standardization; **HSA**, Health Science Authority; **NMPA**, National Medical Products Administration; **PMDA**, Pharmaceutical and Medical Device Agency.

The growing focus on medical device cybersecurity regulations has significant implications for medical device manufacturers, healthcare providers, and patients. Manufacturers will need to invest in cybersecurity measures and ensure that their devices meet regulatory requirements to gain market access in China, Japan, and Singapore.[39] Healthcare providers will need to be aware of the cybersecurity risks associated with medical devices and take appropriate measures to protect patient data and ensure patient safety.[40] Patients may also need to be educated about the cybersecurity risks associated with medical devices and how to protect their personal information.

At the same time, there are concerns that overly prescriptive regulations could stifle innovation and slow the development of new medical devices. It will be important for regulators to strike a balance between ensuring cybersecurity and promoting innovation.

Conclusion

This article provides an overview of the emerging medical device cybersecurity regulations in China, Japan, and Singapore, highlighting their key regulations, challenges, and limitations. The article also explores future developments and implications for the medical device industry and patients in these countries and beyond, emphasizing the significance and contribution of the paper.

Overall, this analysis underscores the importance of robust cybersecurity regulations for medical devices to protect patient safety and data privacy and highlights the need for ongoing research to improve these regulations and keep pace with technological advancements. The article provides valuable insights into the emerging medical device cybersecurity regulatory landscape in China, Japan, and Singapore, and the implications for other countries and international organizations.

Abbreviations

CAC, Cybersecurity Administration of China; **CSA,** Cyber Security Agency of Singapore; **DITTA,** Global Diagnostic Imaging, Healthcare IT & Radiation Therapy Trade Association; **HSA,** Health Science Authority [Singapore]; **MHLW,** Ministry of Health, Labor and Welfare [Japan]; **NMPA,** National Medical Products Administration [China]; **PMDA,** Pharmaceutical and Medical Device Agency [Japan]; **SaMD,** software as a medical device; **SBOM,** software bill of materials guidance; **TPLC,** total product lifecycle.

About the authors

Harshita Menon, MS, a regulatory affairs specialist at Merative. She has four years' experience in regulatory affairs, specializing in the medical device sector. Along with her work in software as a medical device, she has a keen interest in artificial intelligence, machine learning and digital health concepts and their global regulation. Menon has a master's degree in regulatory affairs from Northeastern University, Boston, and a bachelor's degree in pharmaceutical science from Delhi University, New Delhi, India. She can be reached at harshita.menon@outlook.com

Ankita Joshi, MS, is a regulatory affairs specialist at ReCor Medical. She has more than four years' experience in the medical device sector and regulatory affairs, specializing in the medical device sector. Joshi's research interests and areas of expertise include the global harmonization of medical device regulations and the regulatory approach for software in medical devices. She has a master of science degree in regulatory affairs from Northeastern University, Boston, an MBA in hospital and healthcare management from Symbiosis International University, Pune, India, and a bachelor of technology in biomedical engineering from DY Patil University, Belapur, India. Joshi can be reached at ank.joshi@outlook.com

Citation Menon H, Joshi A. Emerging medical device cybersecurity regulations in China, Japan, and Singapore. RF Quarterly. 2023;3(2): 57-67. Published online 28 June 2023. https://www.raps.org/News-and-Articles/News-Articles/2023/6/Emerging-medical-device-cybersecurity-regulations

References

References were checked and verified on 24 June 2023.

1. Slabodkin S. FDA warns about Log4j cybersecurity vulnerabilities in medical devices. MedtechDIve. Published 20 December 2021. https://www.medtechdive.com/news/fda-warns-log4j-cybersecurity-risks-medical-devices/611773/
2. Creemers R. China's emerging data protection framework. J Cybersecur. Published 24 august 2022. https://academic.oup.com/cybersecurity/article/8/1/tyac011/6674794
3. [In Chinese] National Medical Products Administration.

Guidelines for the security risk management of medical devices. Dated 2020.
4. Data Security Law of the People's Republic of China. Adopted 10 June 2021. http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml
5. Pharmaceutical and Medical Devices Agency [Japan]. Pharmaceuticals and medical devices safety. June 2020. https://www.pmda.go.jp/files/000235348.pdf
6. Health Sciences Authority [Singapore]. Regulatory guidelines for software medical devices – A life cycle approach. Dated April 2022. 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
7. State Council of the People's Republic of China. Cybersecurity Law of the People's Republic of China [translation]. Digichina website. Effective 1 June 2017. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/
8. [In Chinese]. Technical guidelines for cybersecurity of medical devices (T/CACME 1-2020). Dated 2020.
9. Emergo. China medical device registration and approval. Not dated. https://www.emergobyul.com/services/china-medical-device-registration-and-approval
10. King H. China's digital health regulatory framework for SaMD. Regulatory Focus. Published 30 November 2022. https://www.raps.org/news-and-articles/news-articles/2022/11/chinas-digital-health-regulatory-framework-for-sam
11. [In Japanese] Pharmaceutical and Medical Devices Agency. Guidance on ensuring cyber security of medical devices. https://www.pmda.go.jp/files/000225426.pdf
12. [In Japanese] International Medical Device Regulators Forum. Principles and practices for medical device cybersecurity. PMDA website. https://www.pmda.go.jp/files/000235089.pdf
13. Katagiri N. Assessing Japan's cybersecurity policy: Change and continuity from 2017 to 2020. J Cyber Pol. Published online 13 March 2022. https://doi.org/10.1080/23738871.2022.2033805
14. Williams P, Woodward A. Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. Medical Devices: Evidence and Research. Published 20 July 2015. https://doi.org/10.2147/mder.s50048
15. Emergo. New guidelines from Japanese regulators cover medical device cybersecurity, remanufactured devices and MDSAP reports. Published 11 February 2022. https://www.emergobyul.com/news/new-guidelines-japanese-regulators-cover-medical-device-cybersecurity-remanufactured-devices
16. Lo D. New cyber-security labelling scheme for medical devices in the works. Straits Times. Updated 20 October 2022. https://www.straitstimes.com/tech/tech-news/new-cyber-security-labelling-scheme-for-medical-devices-in-the-works
17. Cyber Security Agency of Singapore. Cybersecurity labelling scheme for medical devices. CSA website. Published 20 October 2022. https://www.csa.gov.sg/News-Events/Press-Releases/2022/cybersecurity-labelling-scheme-for-medical-devices
18. RegDesk. HSA guidance on life cycle approach for software medical devices: Cybersecurity. Dated 22 November 2021. https://www.regdesk.co/hsa-guidance-on-life-cycle-approach-for-software-medical-devices-cybersecurity/
19. Health Sciences Authority [Singapore]. Regulatory guidelines for software medical devices – A life cycle approach. Date April 2022. 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
20. Scott J, et al. Harmonizing cybersecurity for medical devices: International collaboration moves forward. IAPP website. Dated 9 October 2019. https://iapp.org/media/pdf/resource_center/cybersecurity_for_medical_devices.pdf
21. International Medical Device Regulators Forum. About IMDRF. https://www.imdrf.org/about
22. Mulero A. IMDRF takes up cybersecurity premarket reviews, postmarket activities. Regulatory Focus. Published online 26 September 2018. https://www.raps.org/news-and-articles/news-articles/2018/9/imdrf-takes-up-cybersecurity-premarket-reviews-p?feed=-Regulatory-Focus
23. Mulero A. DITTA calls on FDA, Health Canada to take up proposed IMDRF cybersecurity guidance. Regulatory Focus. Published online 21 September 2018. https://www.raps.org/news-and-articles/news-articles/2018/9/ditta-calls-on-fda-health-canada-to-take-up-propo
24. Global Diagnostic Imaging, Healthcare IT & Radiation Therapy Trade Association. DITTA White Paper on cybersecurity: Best practices in the medical technology manufacturing environment. Dated 8 February 2019. https://www.globalditta.org/uploads/media/DITTA_White_paper_on_Cybersecurity_-_Feb._2019_-_Final.pdf
25. Mulero A. DITTA Pinpoints cybersecurity best practices amid IMDRF work. Regulatory Focus. Published online

14 February 2019. https://www.raps.org/news-and-articles/news-articles/2019/2/ditta-pinpoints-cybersecurity-best-practices-amid
26. Al-Faruque F. IMDRF proposes legacy device cybersecurity guidance after stakeholder feedback. Regulatory Focus. Published online 6 May 2022. https://www.raps.org/news-and-articles/news-articles/2022/5/imdrf-proposes-legacy-device-cybersecurity-guidanc
27. Al-Faruque F. IMDRF guidances address cybersecurity, personalized medical devices and surveillance. Regulatory Focus. Published online 13 April 2023. https://www.raps.org/news-and-articles/news-articles/2023/4/imdrf-guidances-address-cybersecurity-personalized
28. King H. China's digital health regulatory framework for SaMD. Regulatory Focus. Published online 30 November 2022. https://www.raps.org/news-and-articles/news-articles/2022/11/chinas-digital-health-regulatory-framework-for-sam
29. Tanabi H. Updates on medical device and IVD regulation in Japan. Paper presented at: 6th India-Japan Medical Products Symposium; 1 February 2023. https://www.pmda.go.jp/files/000250261.pdf
30. Medical Devices Cluster. Guidelines on risk classification of standalone medical mobile applications and qualification of clinical decision support software (CDSS). Health Sciences Authority [Singapore] website. Dated April 2022. https://www.hsa.gov.sg/docs/default-source/hprg-mdb/guidance-documents-for-medical-devices/guidelines-risk-classification-samd-cdss-(2022-apr)-pub68164581f0d548c29794b7c61b3c8dfc.pdf
31. IMDRF Software as a Medical Device (SaMD) Working Group. Software as a medical device: Possible Framework for risk categorization and corresponding considerations. Dated 18 September 2014. https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf
32. Food and Drug Administration. Guidance for the content of premarket submissions for software contained in medical devices. Issued 11 May 2005. https://www.fda.gov/files/medical%20devices/published/Guidance-for-the-Content-of-Premarket-Submissions-for-Software-Contained-in-Medical-Devices---Guidance-for-Industry-and-FDA-Staff.pdf
33. Food and Drug Administration. Global Approach to software as a medical device. Content current as of 27 September 2022. https://www.fda.gov/medical-devices/software-medical-device-samd/global-approach-software-medical-device
34. Center for Devices and Radiological Health. Cybersecurity in medical devices: Quality systems and premarket [guidance]. Current as of 8 April 2022. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
35. OMC Medical. Cybersecurity for medical devices – FDA and EU MDR perspective. Dated 23 August 2022. https://omcmedical.com/cybersecurity-for-medical-devices-fda-and-eu-mdr/
36. European Commission. MDCG 2019-16 – Guidance on cybersecurity for medical devices. Last updated 22 June 2020. https://ec.europa.eu/docsroom/documents/41863
37. Center for Devices and Radiological Health. Postmarket management of cybersecurity in medical devices [guidance]. Current as of 1 October 2018. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices
38. International Organization for Standardization. ISO/IEC 2700 - Information security management systems: Requirements. Published October 2022. https://www.iso.org/standard/27001
39. Biasin E, Kamenjasevic E. Cybersecurity of medical devices: Regulatory challenges in the European Union. In: Cohen I, et al., eds. The future of medical device regulation: Innovation and protection. Cambridge University Press; 2022:51-62. https://www.cambridge.org/core/books/future-of-medical-device-regulation/cybersecurity-of-medical-devices/AC01289C2DB05E44D-0D98A9E66666562
40. Riggi J. The importance of cybersecurity in protecting patient safety. American Hospital Association website. Not dated. https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety