MEDICAL DEVICE SECURITY

PART 1: LANDSCAPE OF GLOBAL REGULATORY GUIDANCE

Michelle Jump & Salwa Rafee

H-ISAC
HEALTH - ISAC

www.h-isac.org

“Both MDMs and HDOs are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance”.

- U.S. Food & Drug Administration

“We feel strengthened, but also concerned, by new regulatory developments in cybersecurity in Europe. Strengthened, because these deliver a clear expectation for vendors and operators. Concerned, because there is no harmonized approach towards security.”

- The European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (COCIR)

“Cybersecurity for medical devices must be considered as part of a layered, holistic security ecosystem.”

- Australian Government, Therapeutic Good Administration

ABSTRACT

The pace of release of cybersecurity guidance for medical devices across the globe has been accelerating over the past few years. Compliance and legal officers, CIOs, and CSOs working for multinational Medical Device Manufacturers (MDMs) and/or Health Delivery Organizations (HDOs) are tasked with interpreting these guidelines; this review is intended to help them navigate the complex landscape. This report provides a summary of guidance documents and directives from major global regulatory bodies, including the United States, European Union countries, Canada, Australia, and Japan. Some regulatory bodies have restricted their guidance to premarket concerns and others have provided guidelines to include postmarket considerations as well.

This report represents the first in a series on medical device cybersecurity compliance and focuses on providing a landscape overview of medical device cybersecurity guidance. Future parts in this series are planned to include a cross-comparison of convergences and trends and specific expectations on standards. The last edition is expected to include a series of interviews with global regulators in order to gain their perspective on market challenges and how the new regulations can help guide industry.

There is no doubt that the connectivity and digitization of medical devices have helped to improve device functionality, expand benefits to patients, and support the integrity of medical records. However, connecting medical devices to networks or the internet exposes them to increased cyber threats that can potentially lead to increased risk of harm to patients. These can include the following:

- Denial of intended service or therapy
- Alteration of device function to directly cause patient harm
- Loss of privacy or alteration of personal health data

Additionally, there are fundamental security interdependencies between medical devices and the networks to which they connect. Cybersecurity for medical devices must be considered part of a layered, holistic security ecosystem. Regulators seek to outline these expectations and their guidance reflects their current thinking.

EVOLUTION OF GUIDANCE DOCUMENTS

Cybersecurity is a global issue that has driven the development of specific regulatory guidance documents in many countries. As more connected medical devices are added to hospital networks, regulators have increased their oversight and scrutiny when reviewing products requesting market approval as well as when monitoring medical devices during the postmarket phase. Starting in 2005 and rapidly increasing in 2018-2019, the global medical device market has seen the launch of new guidance from countries such as the United States, Canada, Australia, and the European Union (Fig.1). This proves challenging to manufacturers trying to balance these expectations. This document is intended to provide some clarity to that landscape.

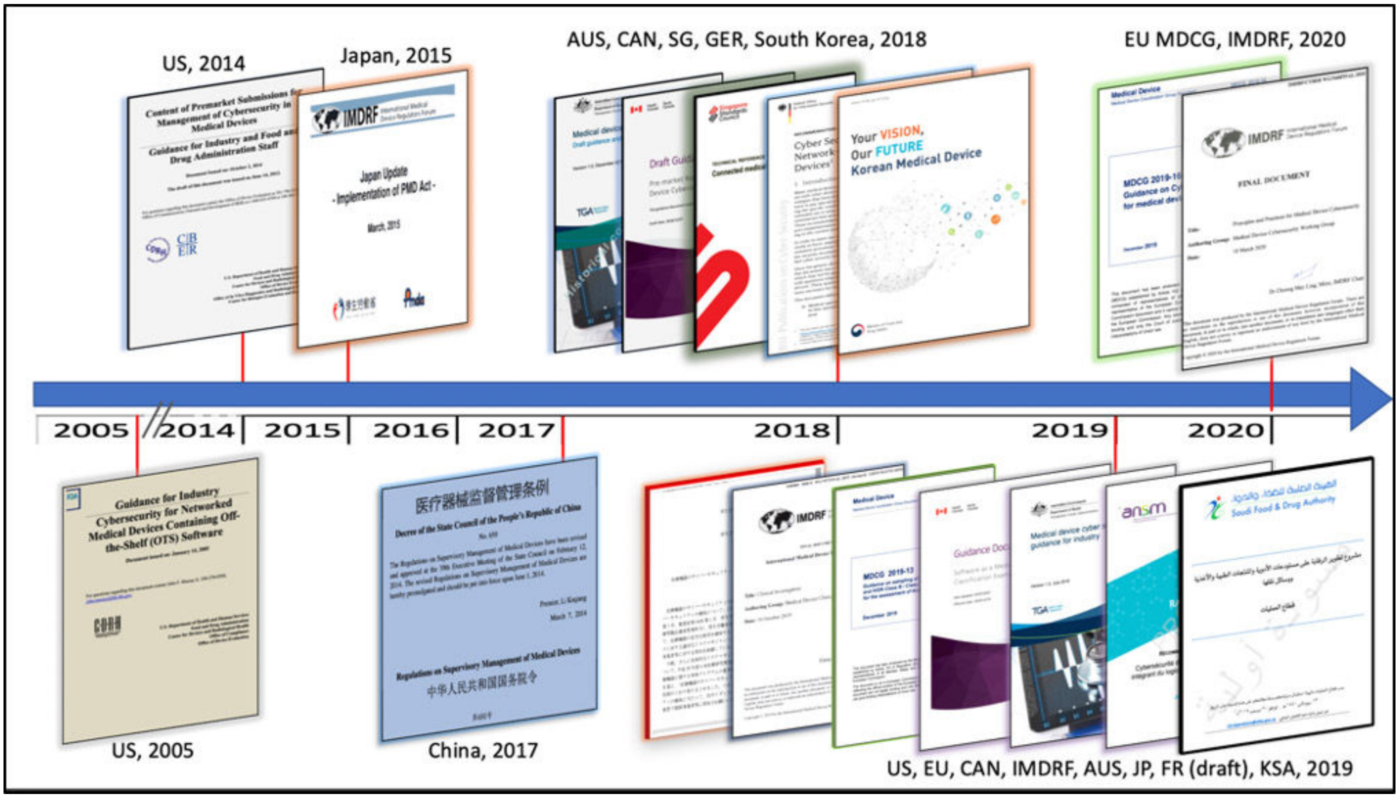

US, 2014
Japan, 2015
AUS, CAN, SG, GER, South Korea, 2018
EU MDCG, IMDRF, 2020
Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
Japan Update - Implementation of PMD Act -
Your VISION, Our FUTURE Korean Medical Device
FINAL DOCUMENT
2005
2014
2015
2016
2017
2018
2019
2020
Guidance for Industry Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software
医疗器械监督管理条例
Regulations on Supervisory Management of Medical Devices
Saudi Food & Drug Authority
US, 2005
China, 2017
US, EU, CAN, IMDRF, AUS, JP, FR (draft), KSA, 2019

Figure (1) showing timeline of documents release year and publishing agencies

The following table shows the pace of release of medical device cybersecurity guidance and highlights the significant increase in guidance release in both draft and final versions in the past several years. Links to these guidance documents, as available, are listed in the bibliography section.

YEAR	COUNTRY	DOCUMENT TITLE
2005	United States	Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (Final)
2014	United States	Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Final)
2015	Japan	Ensuring Cybersecurity of Medical Device: PFSB/ELD/OMDE Notification No. 0428-1 (Final)
2016	United States	Postmarket Management of Cybersecurity in Medical Devices (Final)
2017	China	Medical Device Network Security Registration on Technical Review Guidance Principle (Final)
2018	Germany	Cybersecurity Requirements for Network-Connected Medical Devices
	Japan	Guidance on Ensuring Cybersecurity of Medical Device: PSEHB/MDED-PSD Notification No. 0724-1 (Final)
	Singapore	TR67: Connected Medical Device Security (Final)
	South Korea	Cybersecurity Guide for Smart Medical Service (Final)
	United States	Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Draft)
2019	Australia	Medical device cybersecurity guidance for industry (Final)
	Canada	Pre-market Requirements for Medical Device Cybersecurity (Final)
	France	Cybersecurity of Medical Devices integrating software during their lifecycle (Draft)
	Saudi Arabia	Guidance to Pre-Market Cybersecurity of Medical Devices
	IMDRF	IMDRF Principles and Practices for Medical Device Cybersecurity (Draft)
2020	IMDRF	Principles and Practices for Medical Device Cybersecurity
	European Union	MDCG 2019-16 Guidance on Cybersecurity for medical devices

Table (1) provides a chronological look at the guidance documents as they have been released

This wide variety of guidance documents presents a challenge for global medical device manufacturers who are trying to compile a set of requirements and expectations that would work for their entire market. It is important to start with a general understanding of how each jurisdiction tackles cybersecurity and to summarize its general approach to get a better feel for the main areas of focus.

IMDRF:

The International Medical Device Regulators Forum (IMDRF) was conceived in October 2011 as a forum to discuss future directions in medical device regulatory harmonization. One role of IMDRF is to provide guidelines to regulators across the globe to use when developing their local guidance and regulations. In April 2020, the Medical Device Cybersecurity Working Group published the finalized document; IMDRF Principles and Practices for Medical Device Cybersecurity. The working group is co-chaired by regulatory leaders from Canada and the United States.

The content is comprehensive and represents existing efforts by countries to specify their expectations for medical device cybersecurity. Key elements are outlined up front, including approaching this issue from a Total Product Life Cycle (TPLC) and committing to communication and viewing this as a shared responsibility. This is a foundational concept that ripples through many of the other guidance documents as well as industry initiatives. Security threats are pervasive, and collaboration will be key to effectively battling them. One important point added in this document is that there is also a need for global harmonization. Security threats do not respect man-made borders. Therefore, it is important for each country to approach cybersecurity with a harmonized and thorough approach.

Both premarket (Section 5) and postmarket (Section 6) are addressed in this guidance. The premarket section provides seven (7) high-level design principles such as data integrity and software maintenance. Risk management is also highlighted, providing general expectations of key elements such as security risk assessment, threat modeling, and vulnerability scoring. The Common Vulnerability Scoring System (CVSS) methodology is mentioned as an example of a scoring methodology. Content on security testing and strategies for postmarket management are also included. A robust section on Labeling expectations is also included. Labeling is an important aspect of communication, and regulators appear to see a general weakness in this area and have provided 13 separate recommendations, including the provision of a Software Bill of Materials (SBOM). The remainder of the premarket section covers the type of documentation that regulatory bodies should require for cybersecurity.

While the premarket section primarily addresses medical device manufacturers, the postmarket section includes recommendations for all stakeholders. The section reminds readers that this is a shared responsibility; therefore, expectations for medical device manufacturers is only part of the solution. The importance of information sharing is covered next, including a discussion of the various stakeholders and their roles. The same approach is taken in the Coordinated Vulnerability Disclosure (CVD) section, which outlines a formalized process for collecting and managing cybersecurity vulnerability information from various stakeholders, including researchers. The expectation for manufacturers to establish CVD programs has thus far been restricted mostly to the United States, so it will be interesting to see if this is picked up as a more global expectation.

The postmarket section also includes a section on legacy devices, formally establishing a description as “those medical devices that cannot be reasonably protected against current cybersecurity threats.” This is important because the term “legacy” is used in contextually variable ways. The IMDRF cybersecurity working group has now established its preferred definition for this term to assist in alignment across the industry. As part of legacy device management, the guidance explains, it is important to clearly communicate the end of life (EOL) and end of support (EOS) dates of the devices. This should be done during procurement and installation to avoid unexpected changes to support levels that impact the customer’s ability to provide uninterrupted care.

UNITED STATES

The U.S. Food and Drug Administration (FDA) has been at the leading edge of issuing cybersecurity regulatory guidance, finalizing its first premarket cybersecurity guidance, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" in 2014. This initial effort was fairly straightforward, outlining several general principles, stressing the importance of risk assessment, and aligning its approach with the NIST Cybersecurity Framework, primarily with the high-level stages of identify, protect, detect, respond, and recover. It also included a list of specific documentation expected in a premarket submission, including risk management documentation, traceability matrix of controls, an outline for providing validated software patches, and a summary of controls. Two years later, in early 2016, FDA provided additional guidance on postmarket cybersecurity management, in Postmarket Management of Cybersecurity in Medical Devices, finalizing this guidance later that year. This guidance continues FDA's alignment with the NIST Cybersecurity Framework. It also introduced new concepts and terms such as compensating controls, controlled/uncontrolled risk, and cybersecurity signal. It also introduced the concept of threat modeling and expanded recommendations for security risk management, referencing AAMI's TIR57. The remediation and reporting of cybersecurity vulnerabilities feature prominently and FDA offers an incentive to apply enforcement discretion for reporting requirements under 21 CFR part 806[1] if the manufacturer follows certain requirements for reporting the vulnerability to customers and participates in an ISAO such as H-ISAC[2], meets reporting and response timelines, and the risk meets a defined threshold.

In addition to the national expectations established by the FDA, California has notably signed SB-327 into law, which went into effect in January 2020. This is commonly referred to as the California IoT Security Law and outlines certain expectations for Internet of Things (IoT) devices, including connected medical devices. There are several notable aspects, including the expectation of "reasonable" security features. One of the expectations of "reasonable security" is a unique, preprogrammed password, or requiring a user to generate a new means of authentication prior to initial access being granted. This expectation could prove challenging for some device manufacturers.

The California law does prohibit private parties from suing under California law, however, and delegates enforcement to the California Attorney General, city attorneys, county counsels, and district attorneys.

[1] See 21 CFR 806.10(f)

[2] It should be noted that H-ISAC is referred to its previous name, NH-ISAC, which specified that this organization was focused on "national" efforts. It has since been expanded to a global scope and renamed "H-ISAC."

CANADA

Health Canada released an initial draft of its Pre-market Requirements for Medical Device Cybersecurity for consultation in December 2018 and published the final version on June 17, 2019. At the time of this publication, Health Canada has not yet addressed specific recommendations for postmarket cybersecurity considerations. Health Canada looks for evidence of good cybersecurity management in four categories: (1) Secure Design, (2) Risk Control Activities, (3) Verification and Validation Testing, and (4) Ongoing Monitoring. It also recommends utilizing the U.S. NIST Framework for establishing a cybersecurity management process.

Risk Management also plays an important role in this guidance and Health Canada makes a strong reference to AAMI TIR57:2016 for establishing a security risk management process that is conducted in parallel with safety risk management. Testing recommendations follow very closely with those described in UL 2900-1.

Whereas this is a premarket guidance, the fourth category of evidence expected concerns monitoring and response to vulnerabilities. Health Canada expects evidence that manufacturers have a plan in place to proactively monitor, identify, and address vulnerabilities and exploits as part of their postmarket management because cybersecurity risks to medical devices are continually evolving. It also expects to see a plan that includes patching, vulnerability disclosure, and information sharing.

Lastly, the guidance goes into details regarding labeling, including an expectation for a Bill of Materials (BOM) for all 3rd party and open-source software components. Health Canada uses cybersecurity BOM (CBOM) as a defined term but does not specify this as a requirement in the text. Instead, it uses BOM. Additional information is requested to accompany the BOM, including details related to operation of the device that is intended to reduce or eliminate the cybersecurity risk, logging features, and how the device will update its software.

The following standards are recommended by Health Canada:

1. **AAMI TIR57:2016** – Principles for medical device security – Risk management
2. **ANSI/CAN/UL 2900-1:2017** – Standard for Software Security Network-Connectable Products, Part 1: General Requirements
3. **ANSI/CAN/UL 2900-2-1:2018** – Software Cybersecurity for Network Connectable Products
4. **IEC 80001-1: 2010** – Application of risk management for IT-networks incorporating medical devices
5. **NIST 800-30** Revision 1 Guide for Conducting Risk Assessments, September 2012

EUROPEAN UNION

The Medical Device Coordination Group (MDCG) produced MDCG 2019-16 Guidance on Cybersecurity for Medical Devices, which provides guidance on interpreting the European Union Medical Device Regulation (EU MDR) for cybersecurity. The MDCG is different from the other, more traditional regulatory bodies that have published other medical device guidance documents. They were established by Article 103 of Regulation (EU) 2017/745 and are composed of representatives of all Member States. The MDCG is chaired by a representative of the European Commission. The purpose of the MDCG 2019-16 guidance is to "to provide manufacturers with guidance on how to fulfil all the relevant essential requirements of Annex I to the MDR and IVDR with regard to cybersecurity. However, and in light of the complexity of medical device supply chains and the role played by different operators in ensuring that devices are protected against unauthorized access and possible cyber threats, additional considerations concerning expectations from actors other than manufacturers are provided. And it is formatted as a map to each relevant section. The document was released in January 2020.

The cybersecurity requirements cover both premarket and postmarket aspects, and outline which activities align with each category.

Document notes that several requirements of particular importance to cybersecurity are not explicitly mentioned in the EU MDR, specifically those related to privacy and confidentiality of data associated with the use of medical devices. The MDCG guidance notes that these requirements are associated with other legislations, such as the General Data Protection Regulation (GDPR).

The MDCG guidance does tackle several key aspects of risk management. The term 'Reasonably foreseeable misuse' was introduced as a fundamental concept in ISO 14971 for describing that manufacturers should consider risks if they are assessed as reasonably foreseeable. When manufacturers began to increase their focus on cybersecurity, this concept was often referenced: i.e., Are these cybersecurity risks "reasonably foreseeable" given that the incident rate was very low, and it often required a targeted malicious actor? Section 2.4 in the document states that "any vulnerability which is deemed to be exploitable for a given implementation of software might be discovered and exploited over time and as such should be regarded as an enabler for reasonably foreseeable misuse." This removes the doubt whether cybersecurity risks are really considered reasonably foreseeable misuse.

Section 3 of the document is focused on the overall design and manufacturing process. The design process is centered around "security by design" and "defense-in-depth" practices, which is industry best practice. We see a good representation of these concepts in Figure (2) of the document (shown below). It also aligns with the 19 security capabilities from IEC/ISO TR 80001-2-2.

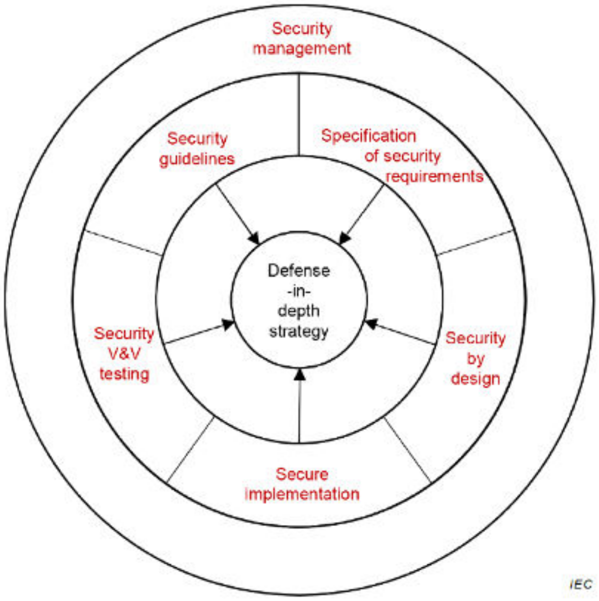


Figure (2) Defense-in-depth (source IEC 62443-4-1)

The concept of risk-benefit analysis, another foundational risk management concept, is addressed in Section 3.5 and is an explicit requirement of the MDR Annex I, sections 1, 2. 3e, and 8. It is aptly specified that not every individual risk must be analyzed for risk-benefit and only an overall Benefit-Risk Analysis is necessary, to include both safety and security hazard categories.

One other notable part of Section 3 is Section 3.6 Minimum IT Requirements. It is notable because the EU MDR Annex I makes an explicit reference to the IT environment hosting the medical device and sets the need to establish minimum requirements. This includes specific expectations for the instructions for use to include minimum requirements for hardware, IT network characteristics, and IT security measures. These requirements do include expectations to meet GDPR-related expectation.

Section 4 covers the documentation and instructions for use requirements. This includes a single reference to a Software Bill of Materials (SBOM) as an example of information that could be included in the Instructions for Use, but it is not explicitly required. The labeling expectations include numerous expectations regarding specific technical details needed to address targeted to IT professionals so that they can effectively install and maintain the medical device in their environment.

The Postmarket section (Section 5) is fairly brief and notes that cybersecurity considerations should be part of the postmarket surveillance (PMS) system. It should be noted that in the EU MDR language, incidents are considered “any malfunction or deterioration in the characteristics or performance of a device made available on the market”. This is compared to a serious incident that led or could have led to death, serious deterioration or a serious public health threat. This is distinct from how “incident” is often used in postmarket vulnerability management.

FRANCE

ANSM (Agence nationale de sécurité du Médicament et des produits de santé) NSM (Agence nationale de sécurité du Médicament et des produits de santé) released its draft guideline titled Cybersecurity of medical devices integrating software during their life cycle in July 2019. The focus of this guideline is for what ANSM refers to as medical devices integrating software (MDIS), which includes both connected medical devices and software as a medical device (SaMD), also called medical device software programmes in this guideline. It also serves as an interpretive guideline for the cybersecurity expectations specific to Annex I of the EU MDR, though the current MDCG 2019-16 should be considered the primary source for interpreting Annex I requirements.

The relationship between safety and security is discussed at length and the guideline provides some valuable discussion on the intersection of this space by the medical device, as can be seen in Figure (3), stressing the need to perform risk management of the information system security (ISS) as well as via ISO 14971.

The guideline includes 64 general provisions to guide software design and maintain secure medical devices. These general provisions cover the total product lifecycle.

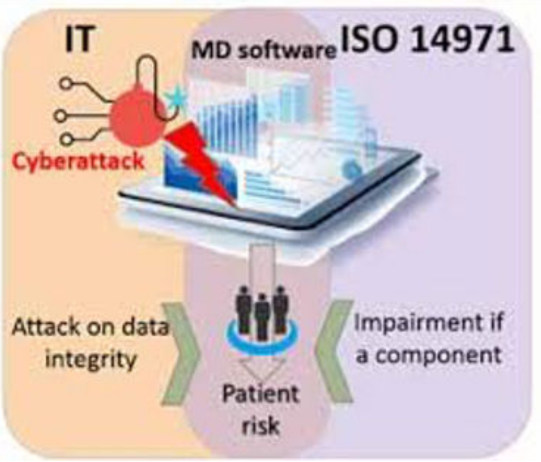


Figure (3) The relationship between safety and security (source ANSM Cybersecurity of medical devices integrating software during their life cycle)

GERMANY

The Federal Office for Information Security published the “Cybersecurity Requirements for Network-Connected Medical Devices” in November 2018, to address security issues with connected medical devices for the MDMs in particular. Special considerations were highlighted for device design, development and product life cycle as it relates to cybersecurity challenges with the intended use of the device (related to patient safety), and best practices for manufacturers to adopt. These recommendations align with regulatory requirements and intend to support implementation and maintenance at an appropriate level of cybersecurity.

These cybersecurity recommendations provide detailed practical assistance on how the identified cybersecurity issues can be reduced. This draws attention to the criticality of performing risk analysis during the conformity assessment procedure for each device category; any identified risks must be reduced and documented.

The document differentiates between the following operating modes:

a. **Medical operation mode:** according to intended medical purpose

b. **Configuration of the device:** The device is being configured for its medical purpose. This includes both cybersecurity configurations that ensure a secure technical operation as well as the settings necessary for medical operation mode

c. **Technical maintenance:** Whereas updates from the manufacturer or third-party providers are being installed and necessary basic calibrations or adjustments are being made

From a cybersecurity point of view, however, there is no clear separation among these operating modes. If, for example, malware has been installed on a software-supported device in technical maintenance mode, this can have an impact on the setting of medical operation mode, according to the intended medical purpose, even if the device has no network-connection in this mode. For this reason, all recommendations are always valid in all operating modes. This document differentiates among operating modes only to enable manufacturers to discern the purpose of the recommendations more easily.

AUSTRALIA

The Australian Therapeutic Goods Administration (TGA) provides three different guidance documents across several stakeholder groups. These include the following:

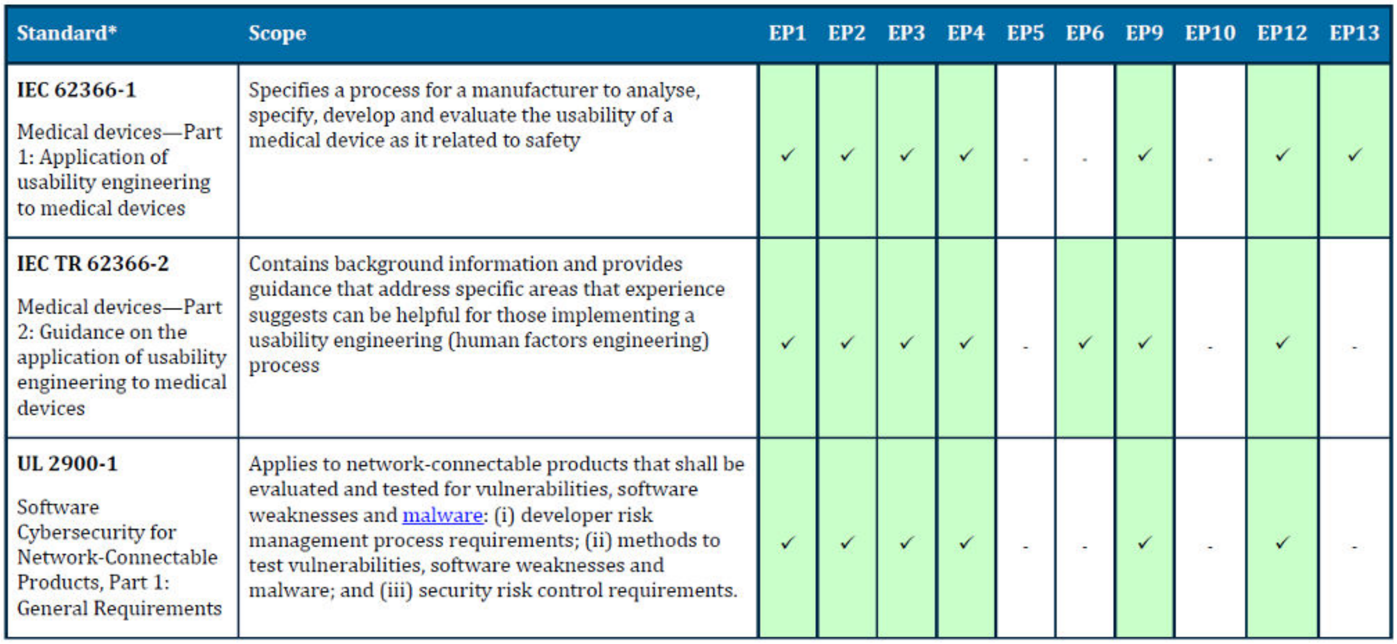
1 Industry

2 Consumers

3 Users

This discussion will focus solely on the industry document, “Medical Device Cybersecurity Guidance for Industry”. As with many of the other global guidance documents, it takes a Total Life Cycle approach, basing its foundation on four categories: (1) risk management procedures, (2) change management procedures, (3) design procedures, and (4) complaint management procedures. A common thread for all these categories is the fact that clinical use is often longer than the expected lifespan of technology and that manufacturers need to plan for this and minimize risk.

The TGA’s approach to the regulations of medical devices is not focused on a prescriptive list of requirements, rather a list of high-level principles to allow for flexibility. These are called Essential Principles. Detailed tables are provided, which map each standard to the specific Essential Principle(s) that it can help fulfill, see table (2).



Standard*	Scope	EP1	EP2	EP3	EP4	EP5	EP6	EP9	EP10	EP12	EP13
IEC 62366-1 Medical devices—Part 1: Application of usability engineering to medical devices	Specifies a process for a manufacturer to analyse, specify, develop and evaluate the usability of a medical device as it related to safety	✓	✓	✓	✓	-	-	✓	-	✓	✓
IEC TR 62366-2 Medical devices—Part 2: Guidance on the application of usability engineering to medical devices	Contains background information and provides guidance that address specific areas that experience suggests can be helpful for those implementing a usability engineering (human factors engineering) process	✓	✓	✓	✓	-	✓	✓	-	✓	-
UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	Applies to network-connectable products that shall be evaluated and tested for vulnerabilities, software weaknesses and malware: (i) developer risk management process requirements; (ii) methods to test vulnerabilities, software weaknesses and malware; and (iii) security risk control requirements.	✓	✓	✓	✓	-	-	✓	-	✓	-

Table (2) Excerpt from the Essential Performance Tables that map to standards (source Medical Device Cybersecurity Guidance for Industry)

General Considerations	Technical Considerations	Environmental Considerations for Intended use	Physical Considerations	Social Considerations
such as the development approach; administration protocols; application of standards; risk management strategies; supply chain management; and provision of information for users	such as cybersecurity penetration testing; modularized design architecture; operating platform security; and Trusted access content provision	such as connecting to networks, and uploading or downloading data	such as mechanical locks on devices and interfaces, physically securing networks, waste management (preventing capture of sensitive paper-based information)	such as designing out or minimizin social-engineering threats (e.g., phishing, impersonation, baiting, tailgating)

Table (3) Premarket highlights from Medical Device Cybersecurity Guidance for Industry

SOUTH KOREA

On July 2, 2018, South Korea's Ministry of Science and ICT has published new guidelines for medical device cybersecurity risk management. The guidelines reference UL 2900, US FDA cybersecurity guidance, and related standards and recommendations in place in other medical device markets. Although the guidelines only provide recommendations to medical device manufacturers and healthcare providers for managing cybersecurity risk, they are expected to pave the way for full-blown cybersecurity regulations from the Ministry for Food and Drug Safety (MFDS) and other South Korean agencies in the near future.

By incorporating UL 2900 as well as other established cybersecurity references and standards, e.g., ISO/IEC 27002, NIST 800-53, and FDA cybersecurity guidance documents, South Korean regulators are indicating a same-page approach regarding recommendations and requirements for MFDS registrants with network-connected devices as well as hospitals and healthcare providers to manage these vulnerabilities.

CHINA

The National Medical Products Administration (NMPA), formerly the CFDA, issued guidelines in 2017 for implementing China's Cybersecurity Law (CSL) in the administration of medical devices in China. As of January 1, 2018, medical device companies are required to register their networked medical devices with NMPA and will be assessed against the Principles on Guiding Technology Examination of Medical Device Cybersecurity Registration. It should be noted that the NMPA guidelines are not mandatory for registration. The applicant conducts a self-assessment and outlines how it has met the CSL. Only Grade II and Grade III medical devices capable of electronic data exchange or remote-control functions via network connection are considered qualified devices and are expected to provide the self-assessment.

When registering, the applicant submits a cybersecurity description file and a cybersecurity instruction manual. Revisions to the application are required when a major cybersecurity update affecting safety or effectiveness is planned. During its review, the NMPA will consider data, technology, and off-the-shelf software. Different protection measures are expected for data characterized as personal or equipment data. When considering technology, NMPA recommends that the applicant follow international and domestic standards to protect their devices. Lastly, the applicant must outline how they are addressing risks related to off-the-shelf software.

The NMPA has also released a draft of a new standard entitled Basic Requirements of Cybersecurity in Medical Electrical Equipment. While not finalized, it does provide some insight on the agency's thinking. This standard leverages several key standards, including IEC TR 80001-2-2:2012, UL 2900-1, UL 2900-2-1, and the MDS2 form. The product characteristics outlined in the standards align with the security capabilities from IEC TR 80001-2-2:2012 and UL 2900-1 and ask for description of these capabilities supported by the device. They also ask for evidence of maintainability.

Appendix A outlines the requirements for conducting a cybersecurity test process and is noted as normative (required). No specific test methods are recommended in the document.

JAPAN

The Pharmaceuticals and Medical Devices Agency (PMDA) released its “Guidance for Ensuring Cybersecurity of Medical Devices” in 2018. This guidance is difficult to find in English translation. It is a short document (9 pages) and focuses on specific cybersecurity measures to be taken by manufacturers to address both premarket and postmarket security of medical devices. A focus for manufacturers should be risk management, stating the guidance, and taking the necessary measures to make those risks acceptable. Off-the-shelf software, including the operating system (OS) are singled out for specific consideration as to its adequacy for the entire lifecycle.

The consideration of security of “secondhand medical devices” (Section 4.1) notes the long service life of medical devices and the challenge that presents for manufacturers and users, particularly when the devices are re-sold, and the traceability becomes challenging. Per this guidance, manufacturers are required to address cyber risk for secondhand devices by providing appropriate instructions for distributors. Equally, distributors are required to provide how they plan to handle cyber risks of these secondhand medical devices.

SINGAPORE

The Technical Reference (TR) published in 2018 was prepared by the Working Group on Connected Medical Device Security appointed by the Technical Committee on Health Informatics under the direction of the IT Standards Committee.

The document is focused on HDOs, and its intent is to build a framework for healthcare institutions and professionals to mitigate the security risks of connected medical devices within the functions of procurement of new devices, and what to include in the requirement documents (such as RFPs). The intent is to ensure that a relevant baseline set of security requirements, day-to-day operations of existing medical devices within HDOs, and context to discuss the process, contractual and security controls are included when implementing a connected medical device into an enterprise network or when de-commissioning a device from the network.

This approach is rather unique among the documents reviewed in this report, which have sought to regulate the medical devices themselves rather than the procurement process.

SAUDI ARABIA

The Saudi FDA (SFDA) published this guidance in 2019 to "provide fundamental concepts and recommendations on premarket submission in the Saudi market and suggest best practices on how to secure medical devices connected to a network."[3] These measures are intended for the manufacturers to reduce associated risks with the finalized medical device.

This guidance document is applicable to premarket submissions for medical devices including In-Vitro medical devices that contain software (including firmware) or programmable logic as well as software that is a medical device (collectively referred to as "software devices"). SFDA aligns with the regulations of many other countries, stressing the importance of security as a shared responsibility between the manufacturer, regulator, user, and healthcare provider. However, it notes that it is the responsibility of the manufacturers to monitor, assess, and mitigate potential cybersecurity risks throughout the lifecycle of their products, such as security of the design and device risk management (aligning with the NIST "Framework for Improving Critical Infrastructure Cybersecurity"). Risk Management is aligned with ISO 14971 but does not reference AAMI TIR 57.

The document outlines the following topics to be implemented in the premarket submission by MDMs and the mandate to provide evidence of compliance for each:

- Security of the design
- Risk management related to cybersecurity of medical devices
- Standards
- Cybersecurity verification and validation testing
- Traceability Matrix
- Planning for continuous monitoring and maintenance plan
- Labelling or Customer Security Documentation

[3] S MDS – G38 Guidance to Pre-Market Cybersecurity of Medical Devices, SFDA 2019

CONCLUSION

In closing, medical device manufacturers are faced with a variety of expectations for addressing cybersecurity across the globe. There are considerable alignment points wherein regulators highlight similar expectations and the hope is that the recently finalized IMDRF cybersecurity guidance will help to further that alignment.

This document serves as the first in a series planned to tackle the issue of global cybersecurity compliance for medical devices. The series currently includes plans for the following:

- **Part 2:** Trend Analysis of Medical Device Cybersecurity Guidance
- **Part 3:** Standards and Technical Reports
- **Part 4:** Perspective of the Global Regulators

The authors would like to acknowledge and thank **Charles Farlow** for his time, efforts and excellent contributions as a peer reviewer.

REFERENCES

International Medical Device Regulators Forum (IMDRF)

- Principles and Practices for Medical Device Cybersecurity (2020) http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf

United States

- Final Guidance: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (2005): https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-networked-medical-devices-containing-shelf-ots-software
- Final Guidance: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (2014) https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0
- Final Guidance: Postmarket Management of Cybersecurity in Medical Devices (2016) https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices
- Draft Guidance: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (2018) https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices

European Union

- MDCG 2019-16 Guidance on Cybersecurity for medical devices (2020) https://ec.europa.eu/docsroom/documents/38924
- France: Cybersecurity of Medical Devices integrating software during their lifecycle (2019) https://www.ansm.sante.fr/S-informer/Points-d-information-Points-d-information/L-ANSM-lance-une-consultation-publique-sur-un-projet-de-recommandations-pour-la-cybersecurite-des-dispositifs-medicaux-Point-d-information
- Germany: Cybersecurity Requirements for Network-Connected Medical Devices (2018) https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_132E.html?nn=6656412

Canada

- Guidance Document: Pre-market Requirements for Medical Device Cybersecurity - Summary (2019) https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents/cybersecurity.html

Australia

- Medical device cybersecurity guidance for industry (2019) https://www.tga.gov.au/publication/medical-device-cyber-security-guidance-industry

Saudi Arabia

- Guidance to Pre-Market Cybersecurity of Medical Devices (2019) https://www.sfda.gov.sa/ar/medicaldevices/regulations/DocLib/MDS-G38.pdf

Japan

- Guidance for ensuring cybersecurity in medical devices (2018)
  Japanese Version – https://www.pmda.go.jp/files/000225277.pdf (used a translation provided by Japan Medical Imaging and Radiological Systems Industries Association (JIRA))
  English version of 2015 notification: https://www.pmda.go.jp/english/safety/info-services/devices/0007.html

China

- Medical Device Network Security Registration on Technical Review Guidance Principle (2017) (Official English version not available for download)

Singapore

- TR 67: Connected Medical Device Security (2018)
  https://itsc.imda.gov.sg/standards/singapore-it-standards/

South Korea

- Cybersecurity Guide for Smart Medical Service (2018) https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1383336

AUTHORS

Salwa Rafee

Vice President, Global Development

Health-ISAC

Salwa Rafee is an innovative and internationally recognized SME leading Global Healthcare Cybersecurity & IT Solutions. She works closely with a wide network of Providers, Payers, Pharmaceuticals, Biotech, and Medical Device Manufacturers on IoT / IoMT / OT Security & Regulations, EMR Adoption and Data Privacy, and transformation projects leading to growth, resiliency and profitability. Over 20 years of progressive leadership roles in Strategy Planning, eGovernment and eHealth Innovation, Consulting Services, Partners and Channels, Integrated Solutions and Complex Program Management with a firm commitment to delivery excellence. Salwa holds a Master of Science degree in Biomedical Engineering & Systems from Boston University and had a postgrad fellowship in Medical Sciences from the University of Alberta.

Michelle Jump

Global Regulatory Advisor

MedSec

Michelle Jump is the Global Regulatory Advisor - Medical Device Cybersecurity at MedSec. She is responsible for providing strategic leadership, training, and advisory services to the medical device industry in the area of cybersecurity compliance, global regulations, standards, product security program development, and security risk management. Ms. Jump actively participates in a variety of domestic and international standards, as well as relevant industry and governmental initiatives to support security within the healthcare industry. Ms. Jump holds a Master of Science degree in Regulatory Science from the University of Southern California and a Master of Science degree in Biotechnology from California State University. She is also RAC certified and a Certified HIPAA Administrator.