FDA Taiwan Food and Drug Administration

Guidance for Industry on Management of Cybersecurity in Medical Devices

---

Document issued on April, 2021

The English translation is for reference only.
The Chinese version shall still prevail in actuality.

I. Introduction

The aim of medical device cybersecurity is to address medical device–related security issues resulting from cyber conduct or data transmission. The medical device cybersecurity prevents unauthorized access, modification, misuse, or rejection of medical devices; such unauthorized activities diminish the function of devices and may harm patients. Moreover, medical device cybersecurity prevents unauthorized access or transfer of medical devices to external recipients.

This guidance was formulated to aid industry in ensuring the cybersecurity of medical devices and proposes cybersecurity-related matters that can be considered by the manufacturers during the phases of product design, research and development, application for inspection and registration, and post marketing.

The content of this guidance was formulated by the central competent authority in Taiwan in accordance with existing information. Nonetheless, laws and regulations may not be updated following technological development. Accordingly, the central competent authority may require industry to provide data on cybersecurity verification and assessment outlined in this guidance, depending on the technological features of the product software architecture and design, to ensure the health and safety of public.

The industry shall utilize the updated version of any relevant international standard or any updated version cited by the guidance. Additionally, they shall cite any reference to other medical device cybersecurity–related international standards.

II. Terms and Definitions

1. **Cybersecurity** – Prevention of unauthorized access or modification, misuse, or rejection of medical devices or prevention of unauthorized access or transfer of information related to medical devices to an external recipient.
2. **Confidentiality** – Establishment of measures to ensure that data, information, and system architecture can be accessed and used by only authorized personnel and physical institutions and can be processed at an authorized time and through an authorized method to ensure data and system security. Confidentiality means that only authorized users (i.e., only trusted users) can access the data, information, or system architecture.
3. **Integrity** - Maintenance of accuracy and integrity of data, information, software, and system without improper modification.
4. **Availability** - Timely access and use of data, information, and information systems through expected methods.
5. **Harm** - Physical harm or health damage to the human body (including death) and damage to assets or the environment.
6. **Authentication** – Authentication of users, operating procedures, or installation actions as a prerequisite for permission to access and use medical devices, data, information, or system.

7. **Authorization** – Provision of authority or permission to access and use medical devices.
8. **Threat** - Unauthorized access, information destruction, data disclosure and modification, or service denial that can lead to incidents with adverse effects on devices, organizational operations (including organization mission, performance, image, and reputation), organizational assets, individuals, and other organizations.
9. **Vulnerability** – Information system, system security, internal control, and staff conduct weaknesses that could be exploited by threat sources.
10. **Threat Modeling** - The identification of potential hacking targets and vulnerabilities to optimize the internet, application programs, and cybersecurity, which can yield measures for preventing or eliminating system threats. For medical devices, threat modeling can be used to identify specific products, specific product lines, and leaks and threats in the organizational supply chain that may harm patients; such modeling can thus improve the security of medical devices.
11. **Compensating Control** - Additional measures taken by the manufacturer to replace or replenish the built-in security design of their products. Such control is not part of the original design and can be allocated in the user environment or set up by users to replenish or provide equivalent cyber protection for medical devices.
12. **Controlled Risk** - Residual risk of cybersecurity vulnerability–induced harm in patients that can be reduced to an acceptable level.
13. **Uncontrolled Risk** – Residual risk of harm that cannot be reduced by existing risk mitigation measures or cybersecurity risk compensation measurements.
14. **Cybersecurity Routine Updates and Patches** – Strengthening of medical devices to improve their security and/or modify vulnerabilities to controlled risk of harm in patients. Such modifications do not apply to the reduction of uncontrolled risk in patients. Routine security updates or patches required for improving medical device security include updates in software, firmware, programmable logics, hardware, and device security as well as updates and patches for executing and processing controlled risks during routine scheduled periods. Routine cybersecurity updates and patches are usually considered to constitute an approach for strengthening medical device security; that is, they are used to strengthen security against vulnerabilities to controlled risk and should not be considered as repair processes. Nonetheless, processes that may lead to adverse consequences or even death cannot be considered as part of routine cybersecurity updates and patches.
15. **Cybersecurity Signal** – Information about possible or validated vulnerabilities or misuses in cybersecurity. Such vulnerabilities or misuses can affect medical devices. Cybersecurity signals originate from traditional sources of information, including internal investigations, post-market surveillance, complaints, and security-oriented information sources (e.g., computer/cyber emergency response/readiness teams, threat indicators, and security research fellows). A cybersecurity signal can be identified from the key medical and public health infrastructure; nonetheless, the other key infrastructure signal (i.e., national defense and finance) can also affect medical device cybersecurity.
16. **Exploit** - Conditions which a certain security threat (accidentally or deliberately) causes one or multiple vulnerabilities can not only affect the security or essential performance of medical devices but also damage the connected devices or systems through medical devices.

III. Scope

1. The guidance can be used as reference by medical device manufacturers in manufacturing or research and development. Examples of its applications are outlined as follows (but not limit to):
   (1) It can be used to determine the composition of medical devices, including software (e.g., firmware) or programmable logic.
   (2) It can also be used to design medical device software (including mobile applications).
2. The guidance is not applicable to bodies or institutions responsible for cybersecurity measures, such as medical institutions, medical device operators, maintenance staff, information system administrators, and information system integrators.
   Remarks: According to the guidance "Medical Software Classification” issued by the Ministry of Health and Welfare on December 24, 2020, some types of software programs are excluded from medical devices, such software shall also be excluded from the scope of application for the guidance. Examples of such software include hospital administrative management software, general health management software, and medication record software. The stakeholders with these types of software should refer to the "Cyber Security Management Act" (June 06, 2018) and "Enforcement Rules of Cyber Security Management Act" (November 21, 2018).

IV. Essential Principles

1. To ensure that the security and validity of a medical device is maintained, medical device manufacturers shall adopt a set of cybersecurity control measures to sustain the cybersecurity of medical devices. The devices shall also be subject to routine assessment for cybersecurity risk, and according to the risk assessment results, the devices should follow an appropriate security management procedure. The cybersecurity management plan should concurrently cover the premarket and postmarket stages and the lifecycle (from product design to product end) of products.
2. The maintenance of medical device cybersecurity is the joint responsibility of all stakeholders, including medical device manufacturers, medical device users, medical device maintainers, medical institutions, information system administrators, information system integrators, health and medical information developers, and data software vendors.
3. To prevent unauthorized access, modification, misuse, or rejection that can lead to patient injury or to avoid authorized access to or storage or transfer of confidential data to external recipients, the confidentiality and integrity of medical devices should be maintained to ensure the accuracy and completion of relevant software and data. Such data should not be modified, which can jeopardize patient security. Moreover, medical devices should have availability to ensure that the product performance does not diminish due to cybersecurity issues and that the devices can be promptly accessed and used as expected.
4. Medical device manufacturers shall include cybersecurity-related considerations as part of the design input. In addition, cybersecurity management methods and measures shall be established as part of software validity and risk analysis. The analysis should include the following factors:
   (1) Identify assets, threats, and vulnerabilities.
   (2) Assess the impact of threat and vulnerability on the functionality of medical devices, end users, and patients.
   (3) Assess the likelihood of unauthorized access according to the identified threats and vulnerabilities.

(4) Define risk level and appropriate risk-reduction measures.

(5) Assess residual risks and conditions of acceptable risks.

5. Medical devices should be designed with cybersecurity architectures that enable them to identify, protect, detect, respond to, and recover from cybersecurity threats. Manufacturers should develop, in advance, cybersecurity-related procedures, regardless of the premarket development or postmarket management, when facing cybersecurity threats.

6. Manufacturers can refer to relevant international evaluation indicators when considering how to complete the cybersecurity features of medical devices. Recommended reference sources for information security requirements and information security risk control measures include AAMI TIR57, IEC TR 80001-2-2, IEC TR 80001-2-8, ISO 27000 series, ANSI UL 2900 series, the US National Institute of Standards and Technology, the Open Web Application Security Project, the European Union Agency for Cybersecurity, and the US Healthcare and Public Health Sector Coordinating Council Joint Cyber Security Working Group. Table 1 lists the design principles that can be considered by medical device manufacturers when designing measures or systems for maintaining product information security.

Table 1. Cybersecurity design principles

Design Principles	Description
Secure Communication	Manufacturers should consider how the device is connected to other devices or the internet. The communication interface may include hardwired connections and/or wireless communication systems, such as Wi-Fi, Ethernet, Bluetooth, and USB.
	Manufacturers should confirm the design characteristics of all inputs (not only external inputs) and consider unsafe devices and environments (e.g., devices connected to home networks or old devices).
	Manufacturers should consider how to ensure the security of data transmission between devices to prevent unauthorized access, modification, or replay. For example, manufacturers should determine how to authenticate the communication between devices or systems, whether encryption is required, how to prevent the unauthorized replay of previously transmitted commands or data, and whether terminating the communication after a predetermined time is suitable.
Data Protection	The collecting, processing, and using of personal data by manufacturers must comply with the "Personal Data Protection Act," "Enforcement Rules of the Personal Data Protection Act," and other relevant regulatory requirements and fulfill their duties to protect data.
	Manufacturers must comply with the "Personal Data Protection Act" and other relevant regulatory requirements when transferring personal data across borders or delegating operations to others for processing through the use of cloud services.
	Manufacturers should consider implementing protective measures for security-related data stored on or transmitted

	from devices, such as encryption measures, and passwords should be stored as cryptographically secured hashes.
	Manufacturers should consider adopting risk control measures to protect the message control or sequencing fields in the communication protocol or prevent cryptographic key information from being damaged.
Data Integrity	Manufacturers should evaluate the system-level architecture to design functions that ensure nonrepudiation of data (e.g., supporting audit logs).
	Manufacturers should consider the risk of damage to device integrity, such as unauthorized device software modification.
	Manufacturers should consider control measures (such as the use of antimalware) to prevent viruses, spyware, ransomware, and other forms of malicious code from running on devices.
User Authentication	Manufacturers should consider user access control to validate who can use the device, grant privileges to different user roles, or allow users to gain access through recorded credentials during emergencies. In addition, the same credentials should not be shared between the device and customer. Examples of authentication or access authorization include passwords, hardware keys, software keys, biometrics, or signals that cannot be generated by other devices.
Software Maintenance	Manufacturers should establish procedures for regular updates.
	Manufacturers should consider how to update or control operating system software, third-party software, or open-source software. They should also plan how to respond to software updates or outdated operating environments that are beyond their control (e.g., medical device software running on unsafe versions of an operating system).
	Manufacturers should consider how to update a device so that it is not affected by newly discovered cybersecurity vulnerabilities. For example, they should establish whether the update requires user intervention or is initiated by the device and verify the update to ensure that it will not adversely affect the safety and efficacy of the device.
	Manufacturers should consider implementing code signing or other similar approaches to update the required connection and the authenticity of the connection or update.
Physical Access	Manufacturers should consider taking control measures to prevent unauthorized persons from accessing devices. The control measures may include implementing physical locks, physically restricting port access, or disallowing physical cables that do not require authentication.
Reliability and Availability	Manufacturers should consider designing a device that can detect, resist, respond, and recover from cybersecurity attacks to maintain its basic functions.

V. Principles of Cybersecurity Risk Management

1. Medical device manufacturers shall continue to establish, record, and execute the following procedures during the lifecycle of medical devices: identification of hazard related to medical device cybersecurity, prediction and assessment of related risks, execution of risk control, and monitoring of the effects of various control measures. The aforementioned procedures should include risk analysis, risk assessment, risk control, and information integration of products before and after production. The analysis items include the following:
   (1) Maintenance of Security and Primary Performance
   (2) Identification of Cybersecurity Signals
   (3) Analysis and Assessment of Vulnerability Properties
   (4) Execution of Risk Analysis and Threat Modeling
   (5) Analysis of Threat Source
   (6) Integration of Product and Threat Detection Capacity
   (7) Assessment of Effects of all Products
   (8) Assessment of Compensating Control
   (9) Assessment of Risk Mitigation Measures and Residual Risks
2. Medical device manufacturers shall develop a risk analysis and management system for ensuring product safety and addressing cybersecurity risks. In particular, when one risk management system that is based on results obtained from the analysis of a specific risk produces improved security measures for product design, another risk management system must be used to assess these security measures. The produced security measures can be designed and implemented only when both systems reduce residual risks to an acceptable level.
3. Medical device manufacturers shall draft the "Cybersecurity Risk Management Plan" prior to executing the cybersecurity risk analysis. The plan shall outline the following content for terms and definitions:
   - Methods of risk analysis and assessment
   - Identification of acceptable residual risk
   - Execution of risk validation
   - Mechanism of postmarket cybersecurity monitoring
   - Collection of cybersecurity information
   - Routine examination of identified threats and vulnerabilities
   - Disclosure policy for identified security vulnerabilities
   - Software update procedures related to safety and performance
4. The expected purpose and function features related to medical devices cybersecurity should be defined before cybersecurity risk analysis. In addition, the possible threats, vulnerabilities, assets to be protected, and possible negative effects should be identified. Manufacturers shall choose an appropriate analytical method according to product features, such as threat modeling, to identify the vulnerabilities and threats that could harm from the products; accordingly, they shall upgrade the medical device security.
5. The manufacturers shall execute a process with explicit definition and adopt a systematic approach to execute risk assessment to determine whether the cybersecurity vulnerability risk of medical devices is acceptable. Manufacturers shall assess the process with detailed definition and documentation to support the objectivity of cybersecurity risk assessment. During the risk assessment process, the exploitability of cybersecurity vulnerability as well as the severity of patients should be considered. The manufacturers shall also

consider the compensating control and risk mitigation measures when conducting the analysis.

6. The manufacturers shall consider adopting an objective cybersecurity vulnerability assessment tool when assessing the possible means through which medical devices can be exploited due to their cybersecurity vulnerabilities; alternatively, they shall use a similar vulnerability scoring system to determine the demand of response and level of emergency. For example, the common vulnerability scoring system and common vulnerabilities and exposures should consider different factors in the assessment process; in addition, they should provide the scores of different ranks, as indicated in the following reference examples:
    - Attacking vector (physical, local, adjacent, remote network)
    - Attacking complexity (high, low)
    - Authorization requirements (none, low, high)
    - User interaction (no need, need)
    - Scope (change, no change)
    - Confidentiality impact (high, low, none)
    - Integrity impact (none, low, high)
    - Availability impact (high, low, none)
    - Exploit code maturity (high, function, conceptual authorization, unauthorized certification)
    - Ranking modification (no available patch, expedient measure, temporary patch, manufacturer's official patch, undefined)
    - Reporting credibility (verified, reasonable, unknown, undefined)
7. Cybersecurity vulnerability is likely used by others; thus, the manufacturers shall establish severity assessment procedures for patients. Several methods are available for executing such assessments, such as the qualitative system proposed by ISO 14971 for assessing harm severity:

Common Terms	**Possible Description**
Negligible:	Results in inconvenient or temporary discomfort.
Minor:	Results in temporary injury or impairment without the requirement for professional medical intervention.
Serious:	Results in injury or impairment requiring professional medical intervention.
Critical:	Results in permanent impairment or life-threatening injury.
Catastrophic:	Results in patient death.

8. The main purpose of cybersecurity vulnerability risk assessment is to examine whether the patient's harm risk is controllable (acceptable level) or uncontrollable (unacceptable level). A combination matrix should be adopted to display the relation between "Likelihood of Vulnerability Used (Exploitability)" and "Severity," which can be applied to assess the risk level and harm caused by cybersecurity vulnerability and the assessment tools for "controlled risks" or "uncontrolled risks," as indicated in the following reference example:

Severity of Patient Harm (if exploited)

Exploitability	Negligible	Minor	Serious	Critical	Catastrophic
High		🟥	🟥	🟥	🟥
Medium			🟥	🟥	🟥
Low					🟥

VI. Cybersecurity Testing

All cybersecurity risk control measures shall be verified and validated against design specifications and design requirements. The related international standards mentioned in IV. Essential Principles are recommended references for cybersecurity testing.

The Manufacturers shall conduct a proper validity test on the cybersecurity mechanism of medical devices (e.g., conduct malware testing on program codes to ensure that the software does not hide the potentially known hazardous risk, and conduct malformed input testing using the data input through an external interface to verify the maintenance of normal operation under random or accidental input). The Manufacturers can also consider implementing structured penetration testing, the objective of which is to attempt to evade risk control measures and security maintenance configurations in order to invade the service system, equipment, and other product-related hardware/software and identify various potential vulnerabilities. This can help verify whether the product data and functions can be stolen or damaged and assess whether the software system and hardware security require improvement.

The types of tests that can be considered by the manufacturers during the verification and validation process are listed in Table 2.

Table 2. Example of cybersecurity testing

Test Category	Test Description
Vulnerabilities and Exploits Testing	Known Vulnerability Testing: Software programs are tested against a database of known vulnerabilities (e.g., the National Vulnerability Database).
	Malware Testing: Malware detection tools are used to scan the program to determine whether any known malware exists.
	Malformed Input Testing (i.e., FUZZ Testing): The device is subjected to massive amounts of malformed tokens (invalid or unexpected inputs) to observe whether the device behaves abnormally or "crashes."
	Structured Penetration Testing: This type of testing requires cybersecurity experts who are familiar with hacking techniques (e.g., white hat or ethical hacker). Cybersecurity experts will attempt to circumvent the defense layers designed inside devices.
Software Weakness Testing	Static Source Code Analysis: Use of a software tool to examine the source code, without executing the software program, for program logic or security design flaws that may cause subsequent security problems.
	Static Binary and Bytecode Analysis: Use of a software tool to analyze and disassemble the code for program logic or

	security design flaws that may cause subsequent security problems.

VII. Premarket Review Requirements

Medical device manufacturers shall clearly record cybersecurity-related activities and submit cybersecurity-related documents when checking registration applications, as presented in Table 3.

Table 3. Cybersecurity-related premarket review requirements

Pre-market Review Information	Description
Design Documentation	Including all interfaces, communication pathways, components (hardware and software), and features designed to mitigate cybersecurity risks associated with patient harm, such as access control, encryption, security updates, logging, and physical security. Please refer to Guidance IV, Essential Principles
Risk Management Documentation	Documentation that describes cybersecurity threats and vulnerabilities, an estimation of the associated risks, description of the control measures in place to mitigate these risks, and evidence to demonstrate that these control measures have been adequately tested. Manufacturers should consider control measures that maximize device cybersecurity while not unduly affecting other security controls. It is recommended to refer to cybersecurity risk management standards (e.g., AAMI TIR57: 2016, AAMI TIR97: 2019, and ISO 14971: 2019 etc.). The risk management document contains the following: ● Comprehensive risk management documentation, such as risk management reports or information security risk management reports, should include threat modeling, identifiable cybersecurity threats, and their vendors (e.g., cloud, chip, and software) that can be used to conduct an information security risk assessment. ● Discussion on the effect of cybersecurity risk mitigation measures on other risk management strategies.
Security Testing Documentation	Test reports that summarize all tests performed to verify the information security of the device and the effectiveness of the mitigation measures. Cybersecurity-related testing data should include specifications (such as the qualification range of each testing and the basis for its formulation), methods, original records, and reports. Please refer to Guidance VI, Cybersecurity Testing Projects.
Traceability Matrix	A traceability matrix that links information security risks, information security control measures, and tests.
Software Bill of Material (SBOM)	The SBOM includes a list of open-source and off-the-shelf software components. The list identifies each software

	component by name, source, version, and build to enable the device users (including patients and health care providers) to effectively manage their assets, understand the potential impact of identified vulnerabilities on the device (and the connected systems), and deploy countermeasures to maintain the safety and performance of the device.
Labeling and Documentation	The following information should be included in the labeling: ● The collection, processing, and use of personal data by various related parties—including medical device manufacturers, medical device users (e.g., medical institutions), information system integrators, health and medical information developers, and data software vendors—in accordance with the requirements of Taiwan's "Personal Data Protection Act." ● Cybersecurity control recommendations for the intended use environment (e.g., antimalware software, network connection configuration, and use of firewalls). ● A list of network ports and interfaces that are expected to receive and send data and a description of port functionality (indicating whether the port is incoming or outgoing and noting that unused ports should be disabled). The following documentation is also recommended: ● Instructions about the backup and recovery functions and the process of restoring the configuration. ● Encryption methods. ● A system diagram presenting all information that the user is required to know.

VIII. Postmarket Cybersecurity Monitoring

1. The manufacturers shall develop a complete postmarket cybersecurity risk assessment plan and documented records, including grievance handling, quality audits, corrective and preventive actions, software validity and risk analysis, and after-sales services.
2. The cybersecurity management plan should include the source of cybersecurity information. The plan should also include a monitoring process performed by a third-party software element to identify new vulnerabilities in the total lifecycle of devices. Accordingly, the manufacturers should develop relevant authentication and validation procedures for software updates and patches to correct the vulnerabilities, including updates and patches related to the software sold on the market. They should constantly endeavor to understand, evaluate, and detect procedures for identifying the existence and influence of cybersecurity vulnerabilities; they should also establish a communication channel with users to collect online hazard messages. Finally, they should adopt risk analysis models, such as threat modeling, to assess methods for developing cybersecurity risk mitigation control measures to maintain product security and performance. Cybersecurity hazard messages are commonly adopted as the basis to develop policy and regulations for mitigating cybersecurity risks, thereby preventing the exploitation of the vulnerabilities.

IX. Hazard Treatment and Reporting Principles

1. Even if residual risks exposing patients to injury are reduced to an acceptable level, manufacturers shall still maintain and enhance the security of the internet environment, which can possibly lower cybersecurity risks. Even if the security risks are at an acceptable level, manufacturers shall still deploy other control procedures as part of the “defense-in-depth” strategy.
2. Routine updates and patches for managing cybersecurity vulnerabilities related to controlled risks can strengthen the security of medical devices. Manufacturers are not required to make application filings, but the competent authority may request that manufacturers provide detailed cybersecurity vulnerability information and routine updates and patches depending on the circumstance.
3. The risks lowering and inadequate compensating control measures can produce uncontrolled risks, which can lead to unacceptable levels of residual risks exposing patients to harm. The manufacturers must resolve uncontrolled risks promptly.

   Because patch programs may not be acquired or implemented on time, the manufacturers shall notify clients and users promptly (within ≤15 days) upon discovering security vulnerabilities. The manufacturers must supply temporary risk control measures as well as develop a plan for reducing residual risks to an acceptable level. The risk control measures must not increase the vulnerability or reduce the validity of devices. The medical device manufacturers shall preserve relevant information in documents, including the processing time and theoretical basis of their corrective plans. In addition, the manufacturers shall at least include the following items in notifications sent to clients and users:

   (1) Describe the security vulnerability, including the possible influence on users as inferred on the basis of existing information.

   (2) Explain the ongoing measures taken to quickly reduce the possible harm to patients.

   (3) If applicable, explain the compensating control measures.

   (4) Explain the commitment toward patching the vulnerability or providing a comprehensive defense strategy to lower the probability and severity of harm. Contact with customers and users and identify when the patch program works should also be provided.

   The manufacturers shall quickly patch the security vulnerability upon knowing the vulnerability, authenticating the correction, and providing the patch program to clients and users, to lower the residual risk to an acceptable level. Under certain circumstances, the compensating control measures can be used as a long-term solution for lowering residual risks to an acceptable level. The control measures must not increase device vulnerability or reduce device validity. Moreover, the manufacturers shall conduct follow-ups with end users, if necessary.
4. If uncontrolled risks cause an adverse reaction, they should be reported to the central health competent authority or the commissioned agency within the period specified in “Regulations for Reporting Serious Adverse Events of Medical Devices”. If the manufacturers assess and determine the possible cause of the adverse reaction, regardless of the severity of the reaction, they should report the information regarding the risks and the corresponding reaction to the central health competent authority or commissioned agency in accordance with the aforementioned regulation.
5. In case of security hazard incidents regulated by the Personal Data Protection Act or other laws and regulations, the manufacturers shall comply with the aforementioned treatment

and reporting requirement for medical device cybersecurity hazard incidents; they should also report and take other necessary treatment according to the relevant law and regulations.

6. Regardless of whether specification or performance updates or modifications are routine or nonroutine, manufacturers shall apply for change and registration in accordance with the "Medical Devices Act" and "Regulations Governing Issuance of Medical Device License, Listing and Annual Declaration."

X. Reference

1. Medical Devices Act
2. Regulations Governing Issuance of Medical Device License, Listing and Annual Declaration
3. Personal Data Protection Law
4. Enforcement Rules of the Personal Data Protection Law
5. Information Security Management Law
6. Detailed Rules for the Implementation of the Information Security Management Law
7. IMDRF: Principles and Practices for Medical Device Cybersecurity, 2020.
8. US FDA: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices- Draft Guidance, 2018.
9. US FDA: Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, 2005.
10. US FDA: Guidance for Industry and FDA Staff: Postmarket Management of Cybersecurity in Medical Device, 2016.
11. US FDA: Guidance for Industry and FDA Staff: Design Considerations and Premarket Submission Recommendations for Interoperable Medical Device, 2017.
12. US FDA: Guidance for Industry and FDA Staff: Deciding When to Submit a 510(k) for a Software Change to an Existing Device, 2017.
13. US FDA: Guidance for Industry and FDA Staff: Guidance for the Content of Premarket Submission for Software Contained in Medical Devices, 2005.
14. Health Canada: Guidance Document: Pre-market Requirements for Medical Device Cybersecurity, 2019.
15. TGA: Medical device cyber security guidance for industry, 2019
16. Saudi Food and Drug Authority: Guidance to Pre-Market Cybersecurity of Medical Devices, 2019.
17. ISO 14971:2019, Medical devices - Application of risk management to medical devices.
18. IEC 80001-1:2010, Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities.
19. IEC/TR 80001-2-2:2012, Application of risk management for IT-networks incorporating medical devices -- Part 2-2: Guidance for the communication of medical device security needs, risks and controls.
20. IEC/TR 80001-2-8:2016, Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2.
21. ISO/IEC 27000 family - Information security management systems.
22. ANSI/AAMI TIR57:2016, Principles for medical device security-Risk management.
23. AAMI TIR 97:2019, Principles for medical device security—Postmarket risk management for device manufacturers.

24. ANSI UL 2900-1:2017, Standard for Software Cybersecurity for Network11 Connectable Products, Part 1: General Requirements.
25. ANSI UL 2900-2-1:2017, Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems.
26. HIMSS/NEMA Standard HN 1-2013, Manufacturer Disclosure Statement for Medical Device Security form (MDS2 16).
27. National Institute of Standards and Technology (NIST): Framework for Improving Critical Infrastructure Cybersecurity.
28. National Institute of Standards and Technology (NIST): Guide for Conducting Risk Assessments, September 2012.