Health Canada Santé Canada

Guidance Document:

Pre-market Requirements for Medical Device Cybersecurity

Date adopted: 2019/06/17
Effective date: 2019/06/26

Canada

Health Canada is responsible for helping Canadians maintain and improve their health. It ensures that high-quality health services are accessible, and works to reduce health risks.

Également disponible en français sous le titre :
Exigences relatives à la cybersécurité des instruments médicaux avant leur mise en marché

To obtain additional information, please contact:

Health Canada
Address Locator 0900C2
Ottawa, ON K1A 0K9
Tel.: 613-957-2991
Toll free: 1-866-225-0709
Fax: 613-941-5366
TTY: 1-800-465-7735
E-mail: publications@hc-sc.gc.ca

Publication date: June 2019

Cat.: H164-278/2019E-PDF
ISBN: 978-0-660-31117-3
Pub.: 190079

Foreword

Guidance documents are meant to provide assistance to industry and health care professionals on how to comply with governing statutes and regulations. Guidance documents also provide assistance to staff on how Health Canada mandates and objectives should be implemented in a manner that is fair, consistent, and effective.

Guidance documents are administrative instruments not having force of law and, as such, allow for flexibility in approach. Alternate approaches to the principles and practices described in this document may be acceptable provided they are supported by adequate justification. Alternate approaches should be discussed in advance with the relevant programme area to avoid the possible finding that applicable statutory or regulatory requirements have not been met.

As a corollary to the above, it is equally important to note that Health Canada reserves the right to request information or material, or define conditions not specifically described in this document, in order to allow the Department to adequately assess the safety, efficacy, or quality of a therapeutic product. Health Canada is committed to ensuring that such requests are justifiable and that decisions are clearly documented.

This document should be read in conjunction with the accompanying notice and the relevant sections of other applicable Guidance documents.

Table of Contents

1. Introduction

Medical devices have evolved from largely analogue, non-networked and isolated hardware to networked devices incorporating remote access, wireless technology and complex software. Increasing levels of interconnectedness and data exchange between medical devices can have significant benefits to both patients and the healthcare system but can also leave devices vulnerable to unauthorized access. These vulnerabilities can negatively impact safety by causing diagnostic or therapeutic errors, or by affecting clinical operations.

The Food and Drugs Act sets out the legislative framework under which medical devices are regulated in Canada. Health Canada as the federal regulator of medical device safety and effectiveness, considers cybersecurity vulnerabilities in medical devices as a potential risk to patients that must be mitigated or eliminated by manufacturers of medical devices.

1.1 Scope and application

This guidance document applies to products that consist of or contain software and are regulated as a medical device (Class I to Class IV) under the Medical Devices Regulations (the Regulations). This includes both in vitro diagnostic (IVD) and non in vitro diagnostic (nIVD) devices.

Manufacturers of all medical devices (Class I to Class IV) should take steps to incorporate cybersecurity considerations into their device related to the design, risk management, verification and validation testing and planning for future events. However, not all considerations will be applicable to every device type.

Class III and Class IV medical devices require a review of submitted evidence of safety and effectiveness before their licence applications are finalized. Therefore, a portion of this guidance document is specific to licensing requirements and outlines the considerations related to cybersecurity in a Class III or Class IV device licence application.

This guidance document should be read in conjunction with the guidance documents (https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents.html) on supporting evidence to be provided for medical device licence applications and licence amendment applications. The content described in this guidance document is to be submitted for review in addition to the general data elements listed in Sections 32(3) and (4) of the Regulations.

Although this document recommends that manufacturers demonstrate in their pre-market licence or licence amendment application that adequate provisions are in place to monitor, prevent, and respond to post-market cybersecurity events, this document does not provide guidance on post-market activities to be performed by the manufacturer.

1.2 Policy objectives

Health Canada considers the inclusion of cybersecurity risk control measures an important consideration in issuing medical device licenses. Therefore, this guidance document provides medical device manufacturers advice on the practices, responses and mitigation measures that can improve the cybersecurity of their device. This guidance also outlines the information to be

submitted as part of a medical device licence or licence amendment application to demonstrate that a medical device, consisting of or containing software, is sufficiently secure from threats that may exploit a vulnerability within a medical device possibly causing harm.

1.3 Policy statements

Health Canada considers cybersecurity a component of the medical device's design and lifecycle that can affect the safety and effectiveness of the medical device. Manufacturers should consider cybersecurity when designing their medical device.

As part of the evidence to demonstrate the safety and effectiveness of a Class III or IV medical device, manufacturers should submit the additional information outlined in this guidance document with their application. Failure to submit the additional information with an application could result in a request for additional information under subsection 35(1) of the Regulations at any time during the review (i.e., during either the screening or review phase).

Risk management is required for all medical devices throughout their lifecycle. Manufacturers should incorporate cybersecurity into the risk management process for every device that consists of or contains software. Manufacturers are also encouraged to develop and maintain a framework for managing cybersecurity risks throughout their organizations.

All cybersecurity risk control measures should be successfully verified and validated against the device's design requirements and/or design specifications. Manufacturers should be able to trace all verification and validation activities back to the device's design requirements and/or design specifications.

1.4 Abbreviations and Definitions

1.4.1 Abbreviations

AAMI
Association for the Advancement of Medical Instrumentation

ANSI
American National Standards Institute

BOM
Bill of Materials

IEC
International Electrotechnical Commission

IMDRF
International Medical Device Regulators Forum

ISO
International Standards Organization

MDB
Medical Devices Bureau

NIST
National Institute of Standards and Technology

TIR
Technical Information Report

TPD
Therapeutic Products Directorate

UL
Underwriter's Laboratories LLC

1.4.2 Definitions

attack is an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

authentication means verifying the identity of a user, process or device often as a prerequisite to allowing access to resources in an information system. [AAMI TIR57: 2016]

availability is the property of data, information and information systems to be accessible and usable on a timely basis in the expected manner (i.e., the assurance that information will be available when needed).

confidentiality means a property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Privacy is a subset of confidentiality.

cybersecurity means the body of technologies, processes, practices, responses and mitigation measures designed to protect a medical device against unauthorized access, modification, misuse, or denial-of-use, and against the unauthorized use of information stored, accessed, or transferred to or from a medical device.

device means an instrument, apparatus, contrivance or other similar article, or an in vitro reagent, including a component, part or accessory of any of them, that is manufactured, sold or represented for use in

(a) diagnosing, treating, mitigating or preventing a disease, disorder or abnormal physical state, or any of their symptoms, in human beings or animals

(b) restoring, modifying or correcting the body structure of human beings or animals or the functioning of any part of the bodies of human beings or animals

(c) diagnosing pregnancy in human beings or animals

(d) caring for human beings or animals during pregnancy or at or after the birth of the offspring, including caring for the offspring, or

(e) preventing conception in human beings or animals

however, it does not include such an instrument, apparatus, contrivance or article, or a component, part or accessory of any of them, that does any of the actions referred to in paragraphs (a) to (e) solely by pharmacological, immunological or metabolic means or solely by chemical means in or on the body of a human being or animal.

hazard means a potential source of harm.

integrity the property of data, information and software to be accurate and complete and have not been improperly modified.

malware means software designed with malicious intent to disrupt normal function, gather sensitive information and/or access other connected systems.

risk means a combination of the probability of occurrence of harm and the severity of that harm. [ISO 13485: 2016]

system means a medical device comprising a number of components or parts intended to be used together to fulfill some or all of the device's intended functions, and that is sold under a single name.

software means a software system that has been developed for the purpose of being incorporated into the medical device being developed or that is intended for use as a medical device in its own right. [IEC 62304:2006]

cybersecurity bill of materials (BOM) means a list that includes but is not limited to commercial, open source, and off-the-shelf software and hardware components included in the medical device that are or could become susceptible to vulnerabilities.

validation means confirmation by examination and the provision of objective evidence that the requirements for a specific intended use have been fulfilled, as set out in the definition of validation in section 2.18 of International Organization for Standardization standard ISO 8402:1994, Quality management and quality assurance - Vocabulary, as amended from time to time.

threat means any circumstance or event with the potential to adversely impact health and safety via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [modified from AAMI TIR57:2016]

threat source means the intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.

verification means confirmation through provision of objective evidence that specified requirements have been fulfilled. [IEC 62304:2006]

vulnerability means a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [AAMI TIR57:2016]

2. Guidance for implementation

Medical device cybersecurity is a shared responsibility between the manufacturer, regulator, user and healthcare provider. Manufacturers are responsible for monitoring, assessing, and mitigating potential cybersecurity risks throughout the lifecycle of their product.

Health Canada recommends manufacturers consider a methodology that addresses cybersecurity risk for its product. The NIST document "Framework for Improving Critical Infrastructure Cybersecurity" is an established framework which may be utilized in whole or in part by the manufacturer as a blueprint of best practices to guide their cybersecurity activities, including those related to risk management. More information on how the framework may apply to medical devices is in Appendix A.

Additionally, a manufacturer must have a strategy to address the cybersecurity risk of a medical device (Class I to Class IV) that runs software code. This strategy should include the following elements.

- Secure design
- Risk management
- Verification and validation testing
- Planning for continued monitoring of and response to emerging risks, vulnerabilities and threats

During the evaluation of Class III and Class IV medical device licence and licence amendment applications, Health Canada will consider these elements in the assessment of the safety and effectiveness of the device. The elements listed above, and Health Canada's expectations with respect to each element, are outlined in the subsequent sections of this guidance document.

2.1 Medical Device Cybersecurity Strategy

2.1.1 Secure Design

Manufacturers should consider cybersecurity early in the product life-cycle when design requirements are being developed. This includes cybersecurity risks and controls when making design choices; and design choices that maximize device cybersecurity while not excessively affecting other safety-related aspects of the medical device (e.g., usability).

Design inputs captured in a requirement specification should include those related to cybersecurity. Addressing cybersecurity risks at the design stage can mitigate the cybersecurity risks that could contribute to: a failure of the medical device in delivering therapy, a breach in the confidentiality, a compromise in the integrity and availability of the medical device data or intentional unauthorized access to the medical device and/or the network. Where applicable, these cybersecurity requirements should be cross-referenced to specific device cybersecurity hazards if the requirements are mitigations to identified hazards. The manufacturer should also consider some design controls that allow the device to detect, resist, respond and recover from cybersecurity attacks.

The following table outlines some design control considerations.

Table 1: Design control considerations

Design Principle	Description
Secure Communications	The manufacturer should consider how the device would interface with other devices or networks. Interfaces may include hardwired connections and/or wireless communications. For each type of interface, the manufacturer should determine the method the device will use to communicate with users (e.g., patients or healthcare professionals), other medical devices/sensors or healthcare systems. Examples of interface methods include Wi-Fi, Ethernet, Bluetooth and USB.

	The manufacturer should consider how data transfer to and from the device is secured to prevent unauthorized modification and disruption. Manufacturers should determine how the devices/systems will authenticate each other.
Data Integrity and Confidentiality	The manufacturer should consider if data that is stored on or transferred to or from the device requires some level of encryption (i.e., the cryptographic transformation of data into a form that conceals the data's original meaning to prevent it from being known or used).
	The manufacturer should consider design controls that take into account a device that communicates with a system and/or device that is less secure (e.g., a device connects to a home network or a legacy device with no device security controls). Confidentiality of patient health information should be a design consideration. Under the Medical Devices Regulations, Health Canada only has authority if a data breach results in patient harm[1].
User Access	The manufacturer should consider user access controls that validate who can use the device. There may also be a requirement for authorization that grants privileges to different classes of users. Examples of authentication or access authorization include passwords, hardware keys or biometrics.
Software Maintenance	The manufacturer should consider how the software will be updated to secure the device against newly discovered cybersecurity threats. Consideration should be given to whether updates will require user intervention or be initiated by the device.
	The manufacturer should determine what connections will be required to conduct updates.
	The manufacturer should consider how often a device will need to be updated via regular and/or routine patches.
	The manufacturer should consider how operating system software, third-party software (e.g., libraries) or open source software will be updated or controlled.
Hardware or Physical Design	The manufacturer should consider controls to prevent an unauthorized person from making physical and software changes

	to the device in order to bypass security controls (e.g., disable a USB port to prevent unauthorized access via USB key).
Reliability and Availability	The manufacturer should consider design controls that will allow the device to detect, resist, respond and recover from cybersecurity attacks.

2.1.2 Device-Specific Risk Management

Risk management is required for a medical device throughout its life-cycle. Manufacturers should incorporate medical device cybersecurity into each device's risk management process, and should develop and maintain an organizational framework for managing cybersecurity risks.

Sound risk management principles, as described in ISO 14971-07:2007 Medical devices – Application of risk management (ISO 14971), should be incorporated throughout the life-cycle of a medical device. Health Canada recommends manufacturers extend these risk management principles to cybersecurity with additional considerations.

Generally, a manufacturer should:

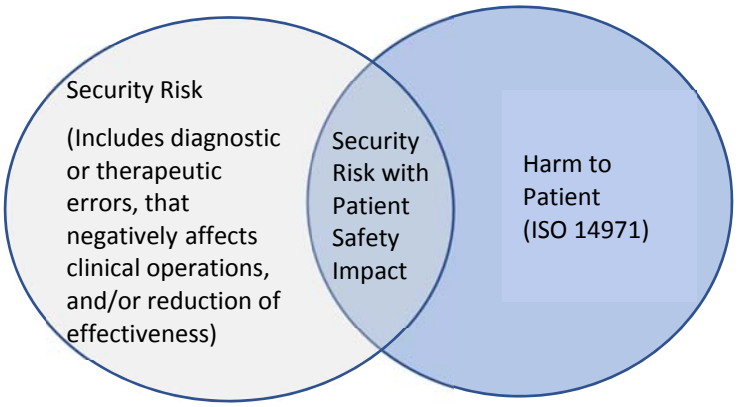
- identify any cybersecurity hazard
- estimate and evaluate the associated risks
- control those risks to an acceptable level
- monitor the effectiveness of the risk controls

As shown in Figure 1, there are cybersecurity risks that may have an impact on the safety or effectiveness of the medical device.

A cybersecurity risk that reduces effectiveness, negatively affects clinical operations, or results in diagnostic or therapeutic errors should be considered in the medical device's risk management process. This consideration is reflected in AAMI TIR57:2016 Principles for medical device security – Risk management which suggests that the risks associated with the cybersecurity of a device can include direct and indirect patient harms (as described in ISO 14971).

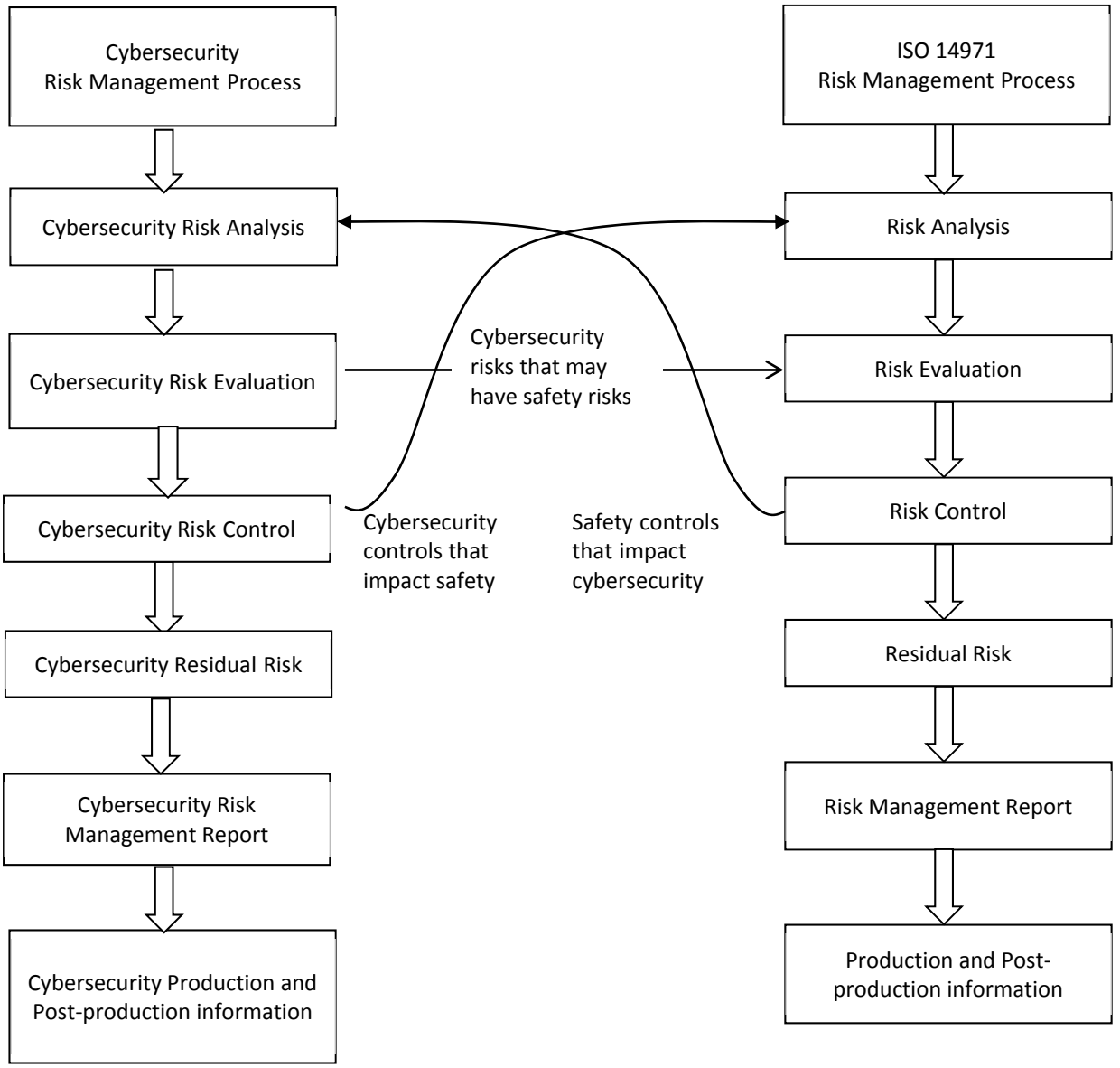
The Venn diagram in Figure 1 illustrates this concept of cybersecurity risk.

Figure 1: A Venn diagram illustrating the relationship between cybersecurity risk and safety risks as defined by ISO 14971 (adapted from AAMI TIR57)



Health Canada recommends that device-specific cybersecurity risk management processes be conducted in parallel to the safety risk management process described in ISO 14971. This parallel process is outlined in Figure 2 and is necessary because of the relationship between safety and security.

Figure 2: An illustration of the relationship between the cybersecurity risk management process and the safety risk management process as defined in ISO 14971 (adapted from AAMI TIR57:2016)



The diagrams in Appendix B outline four examples of the relationship between cybersecurity risk management and safety risk management.

Health Canada recommends the following standards to assist manufacturers conduct their cybersecurity risk management processes in parallel, and potentially iteratively, with their current established risk management process.

- AAMI TIR57:2016 – Principles for medical device security – Risk management
- ANSI/CAN/UL 2900-1:2017 – Standard for Software Security Network-Connectable Products, Part 1: General Requirements
- ANSI/CAN/UL 2900-2-1:2018 – Software Cybersecurity for Network Connectable Products

- IEC 80001-1: 2010 – Application of risk management for IT-networks incorporating medical devices
- NIST 800-30 Revision 1 Guide for Conducting Risk Assessments, September 2012

2.1.3 Verification and Validation Testing

All cybersecurity risk control measures should be successfully verified and validated against design specifications and/or design requirements. Manufacturers should be able to trace all verification and validation activities back to design specifications and/or design requirements.

Testing should include verification and validation of the functions, features and design elements that have been implemented to mitigate identified cybersecurity hazards. Health Canada recommends the UL 2900-1:2017 and UL 2900-2-1:2018 standards for guidance on cybersecurity testing.

The following table outlines the types of testing manufacturers may consider during the software verification and validation process.

Table 2: Types of testing

Test Category	Test Description
Vulnerabilities and Exploits Testing	Known Vulnerability Testing: Software code is tested against a database of known vulnerabilities such as the National Vulnerability Database.
	Malware Testing: Malware detection tools are used to scan the code to determine if any known malware exists.
	Malformed Input Testing (i.e., FUZZ testing): The device is subjected to massive amounts of malformed (invalid or unexpected inputs) to observe if the device will behave in an unorthodox manner or if it will “crash”.
	Structured Penetration Testing: This type of testing requires a cybersecurity expert who is familiar with hacking techniques (i.e., white hat or ethical hacker). The cybersecurity expert attempts to circumvent the layers of defense that were designed into the device.
Software Weakness Testing	Static Source Code Analysis: Utilization of a software tool to examine (i.e., debug) the source code without executing the software code.

	Static Binary and Bytecode Analysis: Utilization of tools that will examine compiled code created from source code.

2.2 Monitoring and Response to Emerging Risks

It is essential that manufacturers proactively monitor, identify and address vulnerabilities and exploits as part of their post-market management because cybersecurity risks to medical devices are continuously evolving. In their pre-market licence application manufacturers should demonstrate a plan for ongoing monitoring of and response to emerging cybersecurity threats to their device. This plan should apply throughout the expected service life.

Considerations in monitoring and responding to emerging risks can include:

- **Post-market vigilance**: A plan to track, assess, and respond to newly discovered vulnerabilities.
- **Patching**: A plan to update the software to maintain the safety and effectiveness of the device either regularly, or in response to an identified vulnerability.
- **Vulnerability Disclosure**: A formalized process for obtaining cybersecurity vulnerability information, assessing vulnerabilities, developing mitigation and remediation strategies, and disclosing the existence of vulnerabilities and mitigation or remediation approaches to various stakeholders.
- **Information sharing**: Participation in Information Sharing Analysis Organizations (ISAOs) or Information Sharing and Analysis Centres (ISACs) that promote the communication and sharing of updated information about security threats and vulnerabilities.

As part of the post-market vigilance strategy, manufacturers should have a process for assessing the exploitability of a cybersecurity vulnerability. In some cases, estimating the probability of a cybersecurity exploit may be challenging due to factors such as the complexity of the exploit, the availability of the exploit, and exploit toolkits. In the absence of data on the probability of the occurrence of harm, conventional medical device risk management approaches suggest using a “reasonable worst-case estimate” or an analysis of exploitability. While these approaches are acceptable, manufacturers should consider using a cybersecurity vulnerability assessment tool or similar scoring system for rating vulnerabilities and determining the need and urgency of the response.

2.3 Medical Device Licence Applications: Cybersecurity Requirements

Class III and Class IV medical device licence and licence amendment applications should include sufficient information for Health Canada to assess the following elements with respect to cybersecurity.

- Secure design
- Risk control activities
- Verification and validation testing
- The plan for on-going monitoring for and action against emerging risks, vulnerabilities, and threats

Details on the general data elements requirements for medical device licence and licence amendment applications are in Guidance Document: Guidance on supporting evidence to be provided for new and amended licence applications for Class III and Class IV medical devices, not including In Vitro Diagnostic Devices (IVDDs) (https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents/guidance-document-guidance-supporting-evidence-provided-new-amended-licence-applications-class-class-medical-devices-including-vitro-diagnostic.html). The following data elements are relevant to cybersecurity:

- Device Labels, Package Label and Documentation
- Marketing History
- Risk Assessment
- Device Specific Quality Plan
- Safety and Effectiveness

Manufacturers may also submit applications in the Table of Contents (TOC) format. Refer to Appendix C for further information regarding the corresponding sections of:

I. Guidance Document on Premarket Requirements for Medical Device Cybersecurity
II. Guidance on supporting evidence to be provided for new and amended licence applications for Class III and Class IV Medical Devices, not including In Vitro Diagnostic Devices (IVDDs)
III. Table of Contents (TOC) folder for submission of Class III and IV licence applications IVD or nIVD

2.3.1 Device Label, Package Label and Documentation

This section should include copies of all labelling, package inserts, product brochures and file cards to be used in connection with the device.

This includes the following information with respect to cybersecurity.

- The cybersecurity BOM which lists all third-party or open source software components that are included in the medical device software. The version and build of the components should be included in the BOM.
- In cases where a risk assessment has determined that further risk controls are necessary, the cybersecurity BOM should include any instructions or information related to:
  - The operation of the device that is intended to reduce or eliminate the cybersecurity risk.
  - Features that protect critical functionality of the device, even during a cybersecurity incident.
  - Backup and restore features.
  - How users download software/firmware, if applicable.
  - Logging features (e.g., syslog, event viewer, application logs, etc.).
  - End of life information.
  - How the device will update its software.
  - How the device can be hardened in its environment (e.g., endpoint protection, software firewall configuration, logging, etc.).

- The intended IT environment the product should be deployed in, and any additional network system controls that must be in place beyond industry standards.

2.3.2 Marketing History

This section should include a summary of reported problems and details of any recalls associated with cybersecurity incidents (e.g., a recall to address vulnerability discovered in a device).

2.3.3 Risk Assessment

Licence applications for both Class III and Class IV devices should include:

- a cybersecurity risk analysis
- a cybersecurity risk management report

The report should also include the risk reduction measures adopted to satisfy safety and effectiveness requirements as described in section 2.1.2 of this guidance document.

2.3.4 Device-Specific Quality Plan

Manufacturers are required to submit a quality plan for a Class IV licence application. The quality plan should demonstrate that a cybersecurity framework is part of the quality standards for the medical device.

2.3.5 Safety and Effectiveness or Performance Studies

Details of any cybersecurity testing that the manufacturer relied on to ensure that the device meets the safety and effectiveness requirements should be included in the Safety and Effectiveness section (or the performance section for IVD licence applications) of the submission. Typically, cybersecurity standards do not have pass/fail criteria and manufacturers should provide the test summaries and/or reports to demonstrate safety and effectiveness with respect to cybersecurity.

2.3.5.1 Standards

A list of all standards applied, in whole or in part, with respect to cybersecurity in the design and manufacture of the device should be included. Evidence that the proposed device is safe and effective should accompany a Declaration of Conformity (https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/forms/declaration-conformity-forms-medical-devices.html) for standards recognized by Health Canada.

2.3.5.2 Cybersecurity Testing

Cybersecurity testing evidence should be provided and include:

- For Class III and Class IV devices a detailed summary of testing that was conducted to verify and validate the security of the device.
- For Class IV devices, reports showing evidence of cybersecurity testing.

2.3.5.3 Traceability Matrix

A traceability matrix should be included that maps all identified cybersecurity risks to:

- Requirement specification(s) (i.e., design inputs)
- Design specification(s) (i.e., design outputs)
- Design verification and validation test(s)

2.3.5.4 Maintenance plan

A summary of the device's maintenance plan should be included. The summary should describe the post-market process(es) by which the manufacturer intends to ensure the continued safety and effectiveness of the device throughout its life-cycle. As described in Section 2.2 of this guidance document, these planned processes may include: post-market vigilance, patching, vulnerability disclosure policies and information sharing.

References

- AAMI TIR57: 2016 Principles for medical device security - Risk management
- ANSI/CAN/UK 2900-1:2017 Software Cybersecurity for Network-Connectable Products, Part1: General Requirements
- ANSI/CAN/UL 2900-2-1:2018 Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems
- Food and Drug Administration (FDA) Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
- Food and Drug Administration (FDA) Post Market Management of Cybersecurity in Medical Devices
- IEC 62304 Medical Device Software - Software life cycle processes
- IEC 62304 Amendment 1 Medical Device Software - Software life cycle processes
- IEC 80001-1 Application of risk management for IT-networks incorporating medical devices - Part 1: roles, responsibilities and activities
- International Medical Devices Regulatory Forum (IMDRF) Software as a Medical Device (SaMD): Key Definitions
- ISO 14971 Medical devices - Application of risk management to medical devices
- National Institute of Standards and Technology (NIST): Framework for Improving Critical Infrastructure Cybersecurity
- National Institute of Standards and Technology (NIST): Guide for Conducting Risk Assessments, September 2012
- Therapeutic Goods Administration - Medical device cyber security v. 1.0, December 2018, Draft guidance for consultation

Appendices

Appendix A - Manufacturers' Cybersecurity Risk Management Framework

Manufacturers should consider the NIST "Framework for Improving Critical Infrastructure Cybersecurity" as a blueprint of best practices to guide their cybersecurity activities, including those related to risk management. Although this document is aimed at improving cybersecurity risk management activities for critical infrastructure, Health Canada supports the framework as a way to improve and maintain the cybersecurity of medical devices.

Health Canada has identified the following five core functions of the framework relate specifically to medical device design controls.

1. **Identify**: The manufacturer should perform a risk analysis to identify cybersecurity risks in their product(s).
2. **Protect**: Design controls should be implemented to limit the risk associated with the identified cybersecurity risks.
3. **Detect**: Processes or measures should be in place to identify when the device has been compromised due to a cybersecurity event.
4. **Respond**: A defined process or plan should be developed on how the device, manufacturer or user will respond to a cybersecurity event.
5. **Recover**: A plan describing the activities the device, manufacturer or user must undertake to restore the device to normal operating capacity following a cybersecurity event. The outcome of any investigations into previous recoveries may be used as feedback into the risk management process.

The framework is intended to complement the ISO 14971 risk management processes. A medical device manufacturer with a mature cybersecurity risk management process is encouraged to utilize the concepts of the framework to identify areas in its cybersecurity risk management processes that can be improved. A manufacturer that does not have an established cybersecurity risk management process may consider using the framework as a guide to establish best practices in the cybersecurity of the devices that they manufacture.

Appendix B - Four Diagrams Outlining the Relationship between Cybersecurity Risk Management and Safety Risk Management

Figure 3: An example of a security risk with no impact on patient safety.

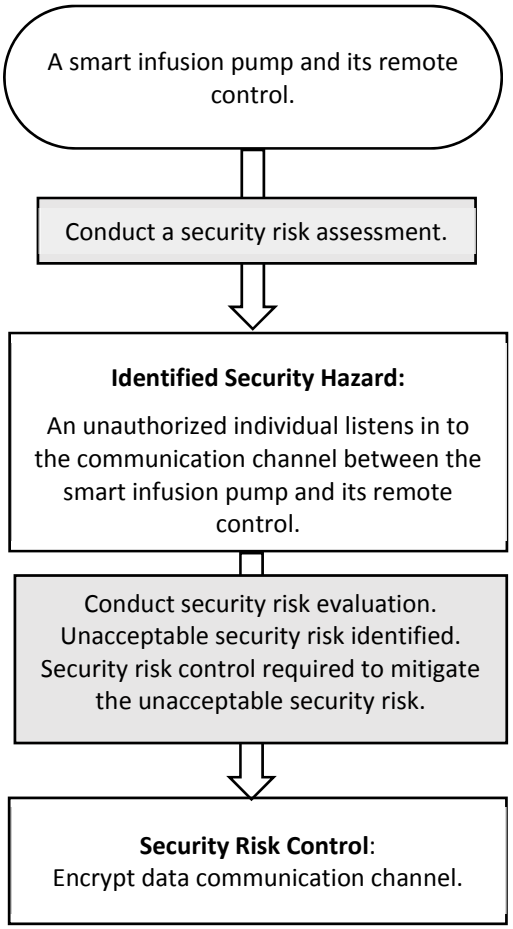


Figure 4: An example of a security risk with an impact on patient safety.

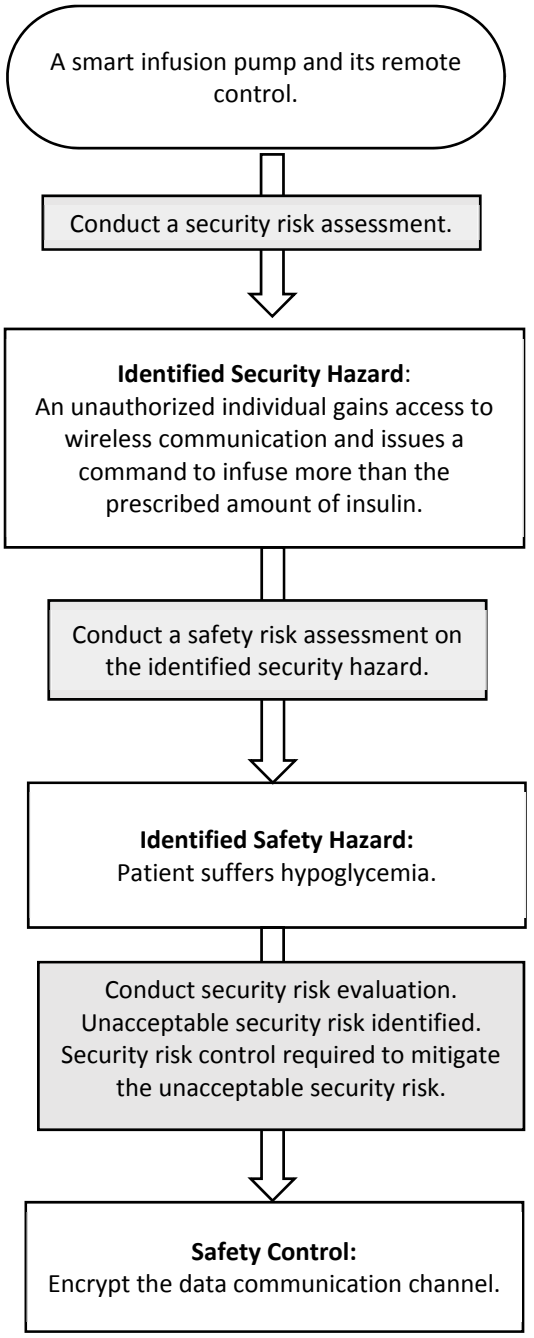


Figure 5: An example of a security risk control with an impact on patient safety.

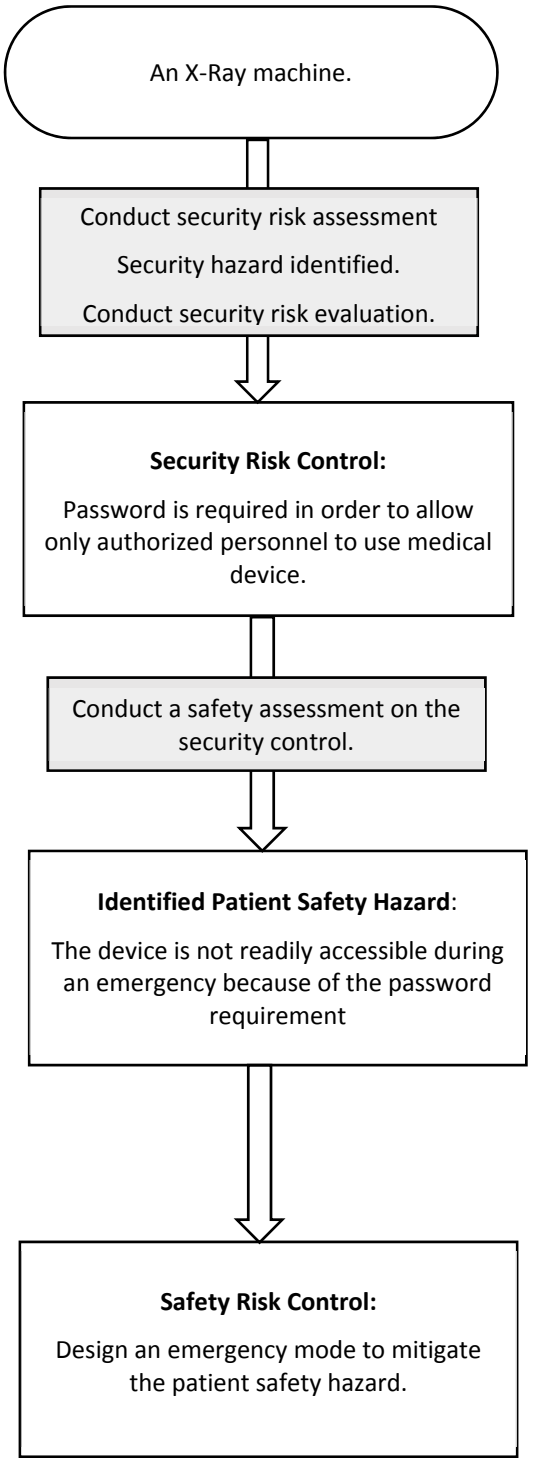
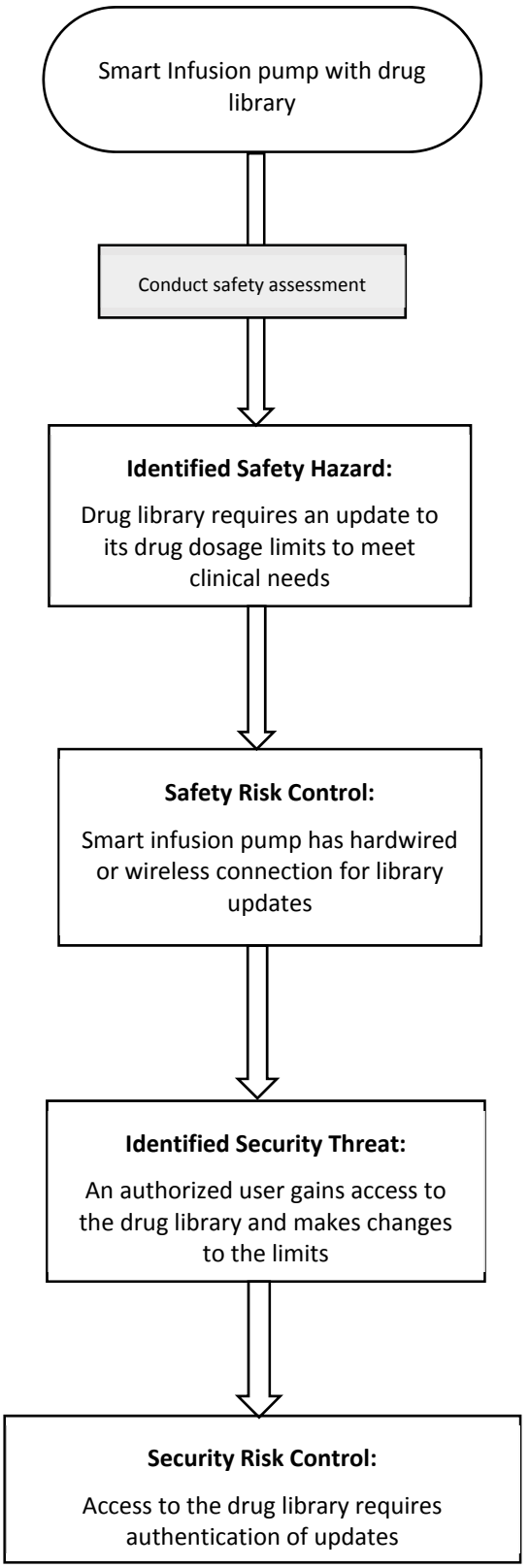


Figure 6: An example of a safety risk control with an impact on security.



Appendix C - Corresponding sections of Health Canada Guidance Document or Table of Contents (TOC) Folder Structure

Guidance Document on Premarket Requirements for Cybersecurity		Corresponding Section of: Guidance on supporting evidence to be provided for new and amended licence applications for Class III and Class IV Medical Devices, not including In Vitro Diagnostic Devices (IVDDs)[2]		Corresponding Section of: TOC Folder Structure[3]
Applicable to Class III and IV Applications				
Section title of Guidance Document Premarket Requirements for Cybersecurity	Section	Class III	Class IV	Class III and IV
Device Labels, Packaging Labelling and Documentation	2.2.1	(3) 4.6	(4) 4.7	5.X
Marketing History	2.2.2	(3) 4.7[4]	(4) 4.8	2.06
Device –Specific Quality Plan	2.2.4	(3) 4.7	(4)4.9.3	6B.05
Safety and Effectiveness or Performance Studies				
Section title	Section	Class III	Class IV	Class III and IV
List of Standards	2.2.1	(3) 5.1	(4) 5.1	3.04
Risk Assessment	2.2.3	(3) 7.0[i]	(4)7.0	3.02
Software Verification and Validation		(3)5.2.2	(4)5.2.2	3.05.05
• Cybersecurity Testing	2.2.5.2	(3) 5.2.2	(4) 5.2.2	3.05.05.11
• Traceability Matrix	2.2.5.3	(3) 5.2.2	(4) 5.2.2	3.05.05.11
• Maintenance Plan	2.2.5.4	(3) 5.2.2	(4) 5.2.2	3.05.05.11

Guidance Document on Premarket Requirements for Cybersecurity (Sections applicable to In Vitro Diagnostic Devices (IVDDs))		Corresponding Section of: IVDD TOC Folder Structure
Section title	Section	Class III and IV
Device Labels, Packaging Labelling and Documentation	2.2.1	5
Market History	2.2.2	2.06
Device –Specific Quality Plan	2.2.4	6B.05 (Class IV only)

Guidance Document on Premarket Requirements for Cybersecurity (Sections applicable to In Vitro Diagnostic Devices (IVDDs))		Corresponding Section of: IVDD TOC Folder Structure
Section title	Section	Class III and IV
List of Standards	2.2.1	3.04
Risk Assessment	2.2.3	3.02
Software/Firmware		3.06.02
Cybersecurity Testing	2.2.5.2	3.06.02.011
Traceability Matrix	2.2.5.3	3.06.02.06
Maintenance Plan	2.2.5.4	3.06.02.011

[1] In Canada, confidentiality of patient health information falls under relevant provincial or territorial legislation (https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/). Additionally, manufacturers should consider if their activities fall under the Personal Information Protection and Electronic Documents Act (PIPEDA) (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/).

[2] For non-TOC applications, Class III and IV licence applications should comply with the format specified in Guidance on Supporting Evidence to be provided for New and Amended Licence Applications for Class III and Class IV Medical Devices, not including In Vitro Diagnostic Devices (IVDDs).

[3] For TOC applications - Please consult the Draft Health Canada IMDRF table of contents for medical device applications guidance for further information regarding the structure and content requirements for applications submitted under the TOC format.

[4] This information is necessary to support the safety and effectiveness related to the cybersecurity of Class III devices.