UNDERSTANDING INTERNATIONAL MEDICAL DEVICE CYBERSECURITY GUIDANCE

Background:
Medical devices are becoming increasingly connected and do not always operate inside the confines of a hospital as, for example, they may be deployed in a home care model. As a result, cybersecurity has become a point of focus for device manufacturers to meet market needs as well as comply with regulatory guidance. Of the top 36 medical device vendors, there are 29 that manufactures devices that are connected to networks. Their connected devices are sold globally, but in a complicated regulatory market, what are the differences in cybersecurity requirements internationally? When designing devices that will operate in hospitals all over the world, how does an MDM prioritize features? Are manufacturers targeting the lowest common denominator? Or perhaps the most rigorous guidance? In reality, the answer will likely lie somewhere in between the two. This whitepaper explores the similarities and differences between four premarket guidance documents from the USA, Canada, Australia, and France.

UNITED STATES

In 2018, the FDA released a draft guidance document, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, which provides cybersecurity recommendations for MDMs. The goals of the guidance are to promote an efficient premarket review process while improving device cybersecurity posture and reducing cyber security risks.

CANADA

Health Canada released a draft guidance, Pre-market Requirements for Medical Device Cybersecurity, in June 2019. Health Canada recognizes the benefits of connected medical devices for patient care and the healthcare system, but that the increasing levels of interconnectedness leave devices vulnerable. Similar to the FDA guidance, the Health Canada document is not law. It is instead intended to provide, based on interpretations of existing regulation, current thinking on improving the cybersecurity of devices along with information to be submitted to demonstrate a device is secure from unauthorized access.

AUSTRALIA

In July 2019, the Australia Therapeutic Goods Administration (TGA) released their version of a premarket guidance, Medical device cyber security guidance for industry. In addition to pre-market guidance, the TGA document also contains total product life cycle (TPLC) guidance, and post-market guidance. This guidance specifies three targeted audiences: medical device software developers, connected medical device manufacturers, and individuals or organizations responsible for the supply of devices in Australia. The purpose is to help MDMs understand how the TGA interprets regulations and how to comply. It should be noted this is a guide that will be updated and evolve over time. Alongside this guidance, TGA produced medical device cybersecurity guidance for users, a guidance for groups or individuals who represent users of medical devices including patients, clinicians, health and IT staff. This guidance highlights that having secure medical devices relies on users as well as manufacturers and assists users in managing cybersecurity risk.

FRANCE

The French Agency for the Safety of Health Products (ANSM) published the draft guidance, Cybersecurity of medical devices integrating software during their life cycle, in July 2019. Referencing Europe's existing regulatory framework for introducing medical devices on the market, the document highlights that there are different interpretations of requirements by MDMs. Due to the increase in medical devices connected to a network, devices are not equipped to deal with the new threats that come with this connectivity. The aim of this guidance is to provide MDMs with recommendations for the early stages of product design to minimize the risk of attack and data compromise.

READERS WILL:

- Learn how other countries organize medical device cybersecurity guidance
- Be able to compare the recommendations for medical device cybersecurity outlined by four international regulatory bodies
- Learn about the scope and differences between the four analyzed documents
- Consider how MDMs may approach differences found in this analysis
- Understand how different regional requirements affect design decisions from a manufacturer's perspective

SECTION I: DATA AND METHODS

Guidance documents from the U.S., Canada, Australia, and France were analyzed to map and contrast requirements. Within each country, requirements that contained related information were included in the same section and were compared to one or more requirements from another international guidance. There are a total of 70 categories that have one or more international guidance requirements (see raw data here). For this analysis, medical device premarket guidance was the focus and note there are other regulatory bodies (e.g. EU General Data Protection Regulation, California Consumer Privacy Act (CCPA)) that have similar expectations for a wider application. It is important to note that because all of the guidance documents analyzed are in draft form at the time of publishing this paper, we expect the documents to evolve going forward.

SECTION II: SIMILARITIES BETWEEN ALL FOUR GUIDANCE DOCUMENTS

SOFTWARE PATCHES AND UPDATES

The FDA, Health Canada, the TGA, and ANSM all have requirements for anticipating software patches. There is a clear consensus that the device should be designed to anticipate patches and updates.

The FDA specifically refers to rapid deployment of patches and updates while the other three guidance documents do not include a component for timing. Additionally, only the FDA asks that devices be designed to facilitate testing of patches and updates.

Health Canada and ANSM similarly consider updating devices throughout their lifecycle, with Canada explicitly including third party/open-source software updates as well.

France takes a more general approach- asking that operating systems are up to date and that the operation of the medical device cannot impair the application of security requirements.

UPDATE AUTHENTICATION

An interesting observation is that while the US calls for authentication of both firmware and software, Australia does not broadly discuss software authentication. This portion of the TGA guidance encourages implementing code signing solely for firmware updates. Conversely, France and Canada only discuss authentication of software, and do not explicitly include language surrounding firmware.

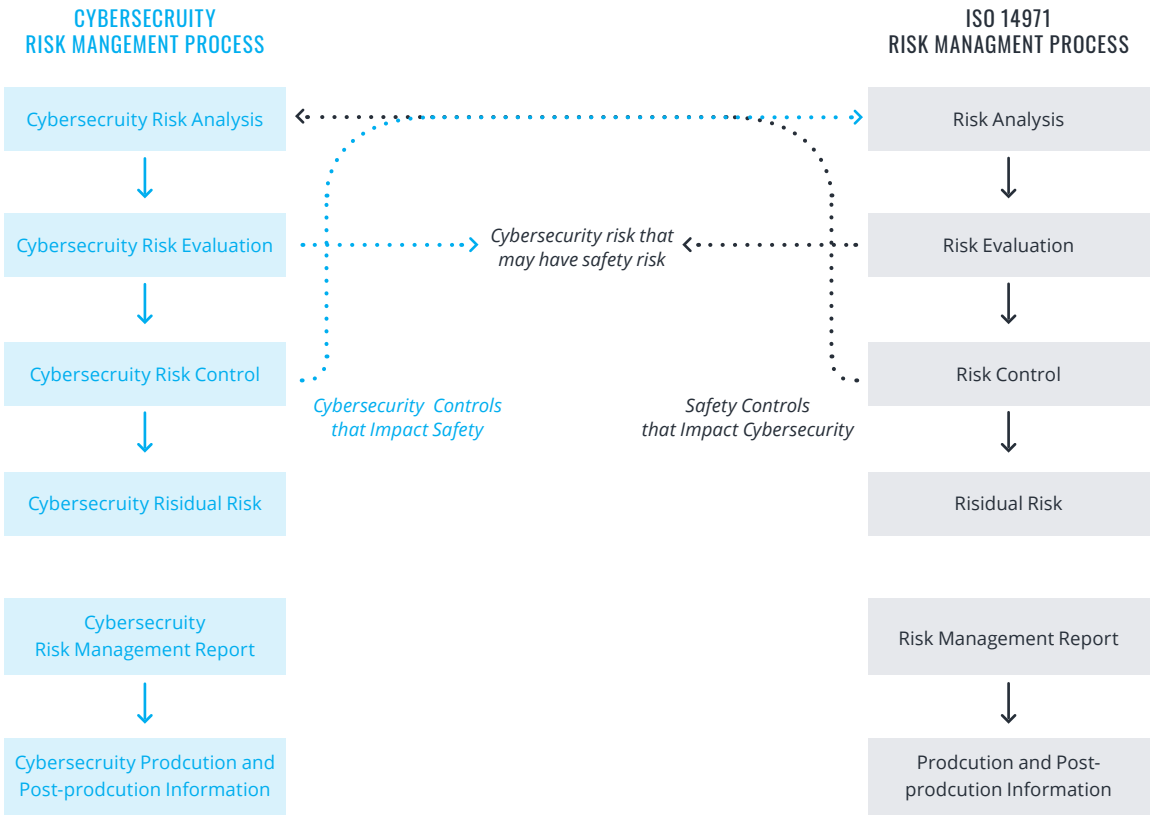
USER ACCESS AND ACCESS CONTROL

Related to the authentication management category above, all four guidance documents analyzed make recommendations for trusted user access and authentication management. Each document supports limiting access to devices by assigning privileges to users based on commensurate job requirements. A notable difference here is that the US includes explicit language around patient safety concerns arising from a cybersecurity incident. The FDA guidance states that a loss of confidentiality of credentials could be exploited and even result in multi-patient harm.

RISK MANAGEMENT AND SECURITY DOCUMENTATION

Requirements regarding security documentation and risk assessment strategies are outlined in each country. The suggested documentation from the FDA is derived from AAMI TIR57 Principles for medical device security- Risk management, a technical information report that illustrates how to apply to security threats the principles outlined in ISO 14971, a standard that specifies a process for MDMs to identify hazards associated with medical devices. ISO (International Organization for Standardization) is an independent, non-governmental international organization that provides document guidelines for a wide range of industries.

Health Canada and the TGA also make references to ISO 14971, to address this category of their standards. Health Canada explicitly recommends following the risk management process described in ISO 14971 (adapted from AAMI TIR57:2016). The parallel is outlined in the figure below:



By providing an illustrative outline of the expected risk management process, Health Canada uniquely structures the expectations for managing the process.

TGA outlines a more flexible risk management process. The TGA suggests manufacturers also consider a risk management strategy that is in line with the US National Institute of Standards and Technology, or NIST, cybersecurity framework. The TGA outlines strategies from both ISO and NIST in the document as potential approaches to risk management.

ANSM takes another approach to risk management and promotes the production of software that is "secure by construction." The requirement asks that MDMs justify the choice of programming language and states that software development will need to comply with encoding rules that allow for automation of vulnerability detection.

ENCRYPT DATA AT REST AND IN TRANSIT

Each guidance document contains requirements regarding encryption of data at rest and in transit. Here, we applaud the FDA for detailing the relevance to patients in stating that a "lack of encryption to protect sensitive information 'at rest' and 'in transit' can expose this information to misuse that can lead to patient harm." Although the FDA is the only regulatory body to explicitly address patient safety in this section, all documents contain an overarching theme of patient safety.

One miss from the FDA that ANSM includes is that the medical device must be relatively autonomous in terms of security (secure network access). This section of the ANSM guidance is not a 1:1 matching to the concept of encrypting data at rest and in transit, however it is a unique requirement in that it implies MDMs must work with HDOs to establish network segmentation. The requirement from France is not as explicit as the other three countries and is more general in that it calls for "encryption of sensitive data" in a broader requirement pertaining to the environment of device use.

THREAT MODELING

All regulatory bodies have requirements regarding cybersecurity hazards and threat modeling. The FDA focuses on considering system level risks and supply chain risks. Health Canada outlines a checklist of general things a manufacturer should do to evaluate and control risk. The TGA asks that MDMs consider cybersecurity practices for manufacturing and the supply chain. ANSM calls for risk analysis, policy for managing and purchasing software components, and verification methods for ensuring there are no vulnerabilities in the software. One difference noted here is that Health Canada does not have language involving the supply chain unlike the other three guidance documents.

MEASURING RISK: EXPLOITABILITY VS. PROBABILITY

A notable difference from the FDA in this section is the use of exploitability versus probability to quantify risk. In the US guidance this risk analysis section focuses on security documentation and recommends providing descriptions of risk leveraging an analysis of exploitability to describe likelihood rather than probability. Health Canada and the TGA also make reference to this concept in the ISO 14971 framework. ANSM does not include requirements regarding exploitability.

CYBERSECURITY TESTING

Each of the four guidance documents contain language surrounding testing, thought with slightly different requirements. The FDA focuses on ensuring there are adequate cybersecurity risk controls. Health Canada focuses on four different kinds of testing: known vulnerability testing, malware testing, malformed input testing, structured penetration testing.

The TGA focuses on implementing penetration testing- with an additional guideline asking that manufacturers take action on the outcomes of the penetration testing.

France also makes an interesting distinction in this guidance. France proposes that dead code, or code that is not specified and not testable, be deleted. Justification must be provided for all lines of code not covered by the tests.

SIMILARITIES BETWEEN GUIDANCE DOCUMENTS FROM HEALTH CANADA, THE TGA AND ANSM

SECURE NETWORK COMMUNICATION

There are a few categories that are covered by Health Canada, ANSM, and the TGA that are not discussed in the FDA draft guidance. The first is the manner in which the medical device is connected to a network.

The requirement from Health Canada and the TGA encourage manufacturers to consider how a device interfaces with other devices or networks. This is something that the FDA has not outlined in the premarket guidance that should be seriously considered. ANSM discusses wireless connections, while Health Canada goes beyond and includes wireless and hardwired connections.

DESIGN CONTROLS AND ENVIRONMENTAL CONSIDERATIONS

In this category, Health Canada states that the manufacturer should consider design controls that take into account a device that communicates with a system or a device that is less secure. A unique addition from Canada is the notion that Health Canada only has authority if a data breach results in patient harm.

The TGA pushes for the provision of information on cybersecurity for users, including plain-language information. As many device users may not have a deep technical understanding of cybersecurity of devices, an aspect of security is providing information for individuals with varying levels of experience or understanding. No other draft guidance provides this kind of requirement.

ANSM states that the connected medical device should be compliant with current good practices requirement when implementing wireless communications. ANSM specifically mentions Wi-Fi mode and refers to the The National Cybersecurity Agency of France (ANSSI) website for good practices for securing Wi-Fi access.

Another related and highly interesting requirement from ANSM suggests the option of using a VPN for greater security within a local network. They provide an example of a medical device used in a patient's home in which the use of a VPN between the device at home and the hospital can help protect the data exchanged.

UNIQUE REQUIREMENTS FROM THE FDA

CRYPTOGRAPHY STANDARDS

The FDA poses two unique requirements for cryptography. The guidance document states that device should contain cryptographically strong authentication and manufacturers should use NIST recommended standards for cryptography or cryptographic protection for communication channels of equivalent strength.

DEVICE SESSION AUTO-TERMINATION

Automatic timed methods be used to terminate sessions in the appropriate environmental conditions.

INCIDENT RESPONSE MANAGEMENT

Devices must be designed to notify users when a potential breach has been detected. The guidance from Health Canada states that the manufacturer should design controls that detect, resist, respond, and recover from cybersecurity attacks, but does not include requirements about notifications when a potential attack is detected.

SOFTWARE CONFIGURATION MANAGEMENT:

The FDA draft guidance document states that the design of the device should enable software configuration management and permit tracking and control of software changes. These changes should also be electronically obtainable by authorized users.

UNIQUE SECURE COMMUNICATION KEY

Each device must have unique, cryptographically secure communication keys to prevent the access of a multitude of devices with knowledge of one key.

CBOM CROSS REFERENCED WITH NATIONAL VULNERABILITY DATABASE (NVD)

Section VII.B.6 is particularly unique to the FDA because it provides criteria for addressing known vulnerabilities and rationale for not addressing remaining known vulnerabilities in accordance with the FDA postmarket guidance.

VARIANT ANALYSIS OF VULNERABILITY

The product life-cycle should facilitate variant analysis of a vulnerability across device models and product lines.

WHITELIST BASED ON DIGITAL SIGNATURE

When feasible, the FDA asks that ensure integrity of software is validated prior to execution, eg. 'whitelisting' based on digital signatures.

WHITELIST BASED ON DIGITAL SIGNATURE

When feasible, the FDA asks that the integrity of software is validated prior to execution, eg. 'whitelisting' based on digital signatures.

UNIQUE REQUIREMENTS FROM HEALTH CANADA

MARKETING HISTORY

This requirement states that there should be a summary of reported problems and details of recalls associated with cybersecurity incidents. There is likely to be some similarity to the FDA Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) database however, Health Canada is the only regulatory body to include this in their pre-market guidance.

UNIQUE REQUIREMENTS FROM THE TGA

Clinician cybersecurity education is only addressed by the TGA. The specific recommendations state that clinicians must also have access to information to understand how and when to apply an update to a device in the case of high risk devices. Other countries do not have clinician education as a part of their guidance, but have encouraged information sharing with clinicians.

UNIQUE REQUIREMENTS FROM ANSM

SOFTWARE DESIGN ACTIVITY

This requirement is particularly interesting due to the language choice used. The term "security by obscurity" relates to not relying on secrecy of design or implementation. It is discussed in other guidance documents, including by the FDA, however, ANSM is the only country to explicitly ban a "security by obscurity" approach in a premarket guidance document.

OPERATION IN FAILSAFE MODE

This requirement urges manufacturers to make available to customers the procedures for using the product in failsafe mode. ANSM asks to pay particular attention to the functional scope in failsafe mode which leads to the question, how practical is it to have a failsafe mode that doesn't hurt functionality? Other considerations listed include performance restrictions, how to enter failsafe mode (i.e. what triggers the mode following a security alert or incorrect operation), and how to exit failsafe mode (via strong authentication).

PRODUCTION LAUNCH AND VALIDATION PROCESS

When integrating outsourced services, an acceptance check system should be put in place prior to integration. ANSM states that the integration of a new element will only be validated after verifying that it satisfies specifications that were defined in advance.

ANSM also states that an acceptance check type approach should be used to manage processes of data imports because it is not feasible to ban data imports outright.

HOSTING

Depending on the nature of Medical Device Integrating Software (MDIS), operating system hardening in order to block or hinder any attempts to execute arbitrary code or illegitimate programs should be implemented or proposed (dedicated memory segments, mutually exclusive permissions for modification and execution, protective mechanisms for the process execution stack, layout randomization for memory storage, etc.).

ISOLATING FROM A NETWORK

From as early as the design phase, and depending on the medical purpose, it is recommended to provide the option of isolating the medical device software from the network or from all communication channels in the event of an attack or threat. This provision should not affect the availability of the device.

SECURE STARTUP

ANSM recommends that connected devices provide an interface used to supply the configuration of the connected medical device system and its operating status.

The devices broadcast information on the network about their own configuration in line with the simple network management protocol (SNMP), a communication protocol used by network administrators to manage devices on the network, and to monitor and diagnose hardware and network problems remotely.

OTHER INTERNATIONAL DOCUMENTS REGARDING MEDICAL DEVICE CYBERSECURITY

The US, Canada, Australia, and France are not the only countries that have released cybersecurity guidance for medical devices. Regulators from Japan, EU, and South Korea have made device security guidance that include more than premarket requirements and have a broader scope than the documents analyzed in this paper, but it is clear that medical device cybersecurity policy is a globally important topic for regulators.

Japan has released a premarket medical device guidance, however it is not publicly accessible in English at the time of publishing this whitepaper. According to the International Medical Device Regulators Forum Open Stakeholder Forum from September 2018, the document entitled, "Guidance for ensuring cybersecurity in medical devices" was released in July 2018 by the Japanese Ministry of Health, Labor, and Welfare.

In July 2018, South Korea's Ministry of Science and Information and Communications Technology (ICT) published guidelines for medical device cybersecurity management. The guidelines entitled, "Cybersecurity Guide for Smart Medical Service" will likely act as a precursor for cybersecurity guidance from the Ministry for Food and Drug Safety and other agencies in South Korea according to Emergo. The guidelines can be found in Korean here.

The Official Journal of the European Union released in April 2017 a document containing Medical Device Regulations that provide a framework for placing and availability of medical devices on the market. The regulations will apply starting May 2020. Although this document is not specific to pre-market requirements for medical devices, it demonstrates the priority of medical device regulations from the EU.

HYPOTHESES

MDMs are not able to 'design for one' in the short term-product versions per country regulation may be the only practical approach.	Manufacturers will need to address the variability of scope and breadth of implementing new features.
With the release of these guidance documents, it is clear that a shift in responsibility is occurring. Rather than the burden of security falling on HDOs, MDMs are expected to take more ownership.	Regardless of size, all medical device manufacturers creating devices that are connected will be held to the same cybersecurity obligation.
There seems to be a fundamental consensus on requirements including patching, user authentication, data encryption, risk management, and threat modeling.	Devices that go home with patients will present operational challenges that must be accommodated in device architecture if similar cyber requirements are to be met.
Guidance encompasses a product lifecycle approach towards security (including development, deployment, maintenance/ operation, disposal).	Emphasis on initial security posture of a device will be important in the short term, but customers and regulators will mandate lifecycle support.
Medical device specific cybersecurity requirements from global regulators will continue to evolve as the industry and ecosystem matures.	The medical device industry must be cautious against over reliance on "security frameworks" and must rapidly iterate to keep up with technology best practices as they emerge.

DISCLOSURES

The authors of this paper are employed by MedCrypt Inc, a medical device cybersecurity software developer.

Thank you.

Axel Wirth, CSS
axel@medcrypt.com

Vidya Murthy
vidya@medcrypt.com

Kate Schneiderman
kate@medcrypt.co

Published Nov, 2019