Australian Government
Department of Health
Therapeutic Goods Administration

Medical device cyber security

Draft guidance and information for consultation

Version 1.0, December 2018

TGA Health Safety Regulation

Confidentiality

All submissions received will be placed on the TGA's Internet site, unless marked confidential. Any confidential material contained within your submission should be provided under a separate cover and clearly marked "IN CONFIDENCE". Reasons for a claim to confidentiality must be included in the space provided on the TGA submission form. For submission made by individuals, all personal details, other than your name, will be removed from your submission before it is published on the TGA's Internet site. In addition, a list of parties making submissions will be published. If you do not wish to be identified with your submission you must specifically request this in the space provided on the submission form.

Contents

Preface

Australia's Therapeutic Goods Administration (TGA) is responsible for the regulation of therapeutic goods within Australia, as defined by the *Therapeutic Goods Act 1989*. The TGA provides a regulatory framework to enable Australians to maintain confidence in existing and emerging health and medical solutions. It achieves this by assessing and monitoring the quality safety and effectiveness of therapeutic goods and the activities associated with their supply. As technology progresses, the capabilities and functionality of medical devices are becoming more interconnected. Software in particular is becoming increasingly important and pervasive in healthcare. As the complexity of devices increases so does the potential for hardware and software vulnerabilities.

In order to support Australia's medical device cyber security capability, the TGA is establishing regulatory guidelines to embed cyber security practices and protocols across the medical device sector (manufacturers, sponsors, clinicians and patients).This guidance will assist in supporting the implementation of risk-based regulatory approval pathways that are guided by, and support, the Australian Government's cyber security strategy[1].

This draft guidance document provides separate information for manufacturer and sponsors and for clinicians and patients. Users of medical devices (clinicians and patients) may wish to focus on Part 2. It is intended that the final guidance documents will be published separately.

We are seeking your feedback on the applicability of the content and on the usefulness of the document. Your feedback will inform the development of final guidelines and the implementation of appropriate regulatory pathways, to protect confidence in the cyber security of existing and emerging medical devices available for use in Australia.

Invitation to comment

Industry, peak bodies, professional and consumer groups and individuals are invited to provide comment on the draft guidance in particular Parts 1 and/or Part 2. The TGA invites submissions by close of business on 14 February 2019. We will use submissions received to help inform the final guidance document.

Please forward all feedback via email to: digital.devices@tga.gov.au.

This is a draft document, and should therefore not be relied upon for advice regarding the regulation of medical devices.

[1] https://cybersecuritystrategy.homeaffairs.gov.au/

Introduction

Connectivity and digitisation of medical device technologies may help improve or increase device functionality. However, the connection of devices to networks or the internet exposes devices to increased cyber vulnerabilities that can potentially lead to unacceptable risk of harm to patients. These include denial of service or intended therapy, alteration of personal health data or alteration of device function so that it can cause actual patient harm.

The Therapeutic Goods Administration (TGA) recognises that to continue providing a clear regulatory environment for connected medical devices, it is essential that medical devices developers, manufacturers, sponsor and users have regulatory guidance concerning requirements for cyber security of medical devices.

Chapter 4 of the *Therapeutic Goods Act 1989* (the Act) provides for the safety and satisfactory performance of medical devices, by setting out particular requirements for medical devices, establishing processes aimed at ensuring those requirements are met, and providing for enforcement of these requirements. The requirements for medical devices includes fifteen 'Essential Principles', set out in Schedule 1 of the Therapeutic Goods (Medical Devices) Regulations 2002 (the MD Regulations), which relate to the safety and performance characteristics of medical devices. Assurance that relevant medical devices are appropriately cyber- secure is required for compliance with a number of the Essential Principles.

Purpose and scope

This document provides draft regulatory guidance on cyber security for medical devices, in line with the existing regulatory requirements. The aim of the document is to provide guidance to:

- manufacturers and sponsors of medical devices that have potential cyber- security risk on pre-market and post-market requirements
- users of medical devices that have cyber security risk on how to reduce that risk.

The guidance is intended for the following:

- Manufacturers that develop software for use in or as standalone medical devices (such as in Software as a Medical Device)
- Manufacturers of medical devices where devices include software components that may have cyber security vulnerabilities
- Medical devices sponsors who are responsible for the supply of medical devices in Australia, to ensure that safety and quality is demonstrated and compliance with the Essential Principles is maintained
- Groups or individuals who represent users of medical devices including:
  - Healthcare professionals who use medical devices to diagnose and treat patients
  - Clinical and biomedical engineers who are responsible for managing medical device assets in a health and medical environment
  - General and IT administrators responsible for systems, procedures and processes in a health and medical service environment
  - Consumers who use a registered medical device under the guidance of their health and medical professional
  - Consumers who use a registered medical device that does not require medical supervision.

Part 1 - Guidance for industry

Medical devices cannot generally be supplied in Australia unless they are included on the Australian Register of Therapeutic Goods (ARTG). Inclusion on the ARTG requires considerations that span the life of a medical device, including:

- pre-market via conformity assessment
- market authorisation via inclusion in the ARTG
- post-market monitoring, and
- end-of-life / withdrawal of support.

Along each stage, manufacturers need to ensure continuing compliance with the Essential Principles. Risk management for medical device cyber security requires assessment and action over the life-cycle of the device and with consideration of the multiple environmental factors that may be applicable. Some considerations include that:

- Medical devices and associated networks they operate in can never be completely cyber secure, and that medical device users themselves represent a potential threat.
- The medical device cyber threat landscape is rapidly evolving and requires constant monitoring and appropriate corrective and preventative action from manufacturers and sponsors.
- Potential harm to patients from an adverse medical device cyber security event would clearly include physical harm to patients (e.g. a device no longer operating as intended). There may also be other consequences for patients arising from a cyber security event related to a medical device, including for example, psychological harm, breaches of privacy through the disclosure of personal information, or financial consequences.
- Clinical use of the device is often considerably longer than the expected lifespan of the technology that allows its operation (e.g. software and connectivity hardware), and this technology receives less frequent patches over time, or becomes officially unsupported.

The assessment of cyber security risk, as with other risks for medical devices, is the responsibility of the manufacturer.

- **Pre-market**: Manufacturers are required to address cyber security risks during the design and development of a medical device. This includes:
  - General considerations, such as the development approach, application of standards, risk management strategies, supply chain assessment and provision of information for users.
  - Technical considerations, such as cyber security performance testing, modularised design architecture, operating platform security, emerging software and Trusted access and content provision.
- **Post-market**: Manufacturers and sponsors are required to continually assess and take action on medical device cyber security risk. This includes understanding cyber security risk, and how to respond to cyber security threats and risks should they occur.

General responsibilities and requirements

The information provided in this section details the general responsibilities and requirements (for both pre and post market consideration) for medical device manufacturers and sponsors to ensure that devices meet regulatory requirements associated with cyber security, specifically risk management frameworks, including:

- Medical device total product life cycle (TPLC) approach
- Medical device cyber security requirements under the Essential Principles
- Standards that will assist manufacturers and sponsors to meet the Essential Principles
- Proactive cyber security risk monitoring, and threat information and intelligence sharing

Total product life cycle (TPLC)

Risk management is expected to be an ongoing activity, which is considered and documented from medical device concept through to obsolescence. Meeting these expectations is most readily achieved by adopting a total product life cycle (TPLC) approach to risk and quality management. As with other risks, if cyber security risk is not effectively minimised throughout the life of the device, it can lead to issues including: a medical device failing to deliver its therapeutic benefit, a breach in the confidentiality, integrity and availability of medical device data, or malicious unauthorised access to the medical device and the network it operates on. Underpinning a TPLC approach is the ongoing application and updating of:

- quality management systems
- risk management procedures
- change management procedures

Essential Principles

A number of the Essential Principles require that a manufacturer minimise the risks associated with the use of the device; this implicitly includes minimisation of cyber security risk.

In particular, Essential Principle 1(b) requires, among other things, that a medical device is to be designed and produced in a way that ensures that any risks associated with the use of the device are acceptable risks when weighed against the intended benefit to the patient, and compatible with a high level of protection of health and safety.

Further, Essential Principle 2(2) requires, among other things, that in selecting appropriate solutions for the design and construction of a medical device so as to minimise any risks associated with the use of the device, the manufacturer must eliminate or reduce the identified risks as far as possible by adopting a policy of inherently safe design and construction, and ensuring adequate protection measures are taken in relation to any risks that cannot be eliminated.

For a medical device to be included on the ARTG, the sponsor must demonstrate compliance with the Essential Principles.

The Essential Principles are not a prescriptive list of requirements for manufacturers to comply with and instead provide flexibility according to the intended use and risk profile or class of the device. The TGA requires that the Essential Principles are met by applying accepted best-practice regarding quality management systems and risk management frameworks, which is typically via application of state of the art standards (See also Part 1, Relevant Standards).

Dealing in medical devices that do not comply with the Essential Principles may have compliance and enforcement consequences; it may be an offence or may contravene a civil penalty provision of the Act[2].

Six general Essential Principles are relevant to all medical devices, and a further nine Essential Principles about design and construction apply to medical devices on a case-by-case basis, depending on the technology used within the device (refer to the MD Regulations - Schedule 1 for more information).

As cyber security vulnerability can be a safety concern, consideration and minimisation of such vulnerabilities and risks are imperative to compliance with many of the Essential Principles and sponsors must be able to demonstrate this compliance. Essential Principle 2, for example, requires minimisation of risks that arise from use of the device for both its intended purposes but also foreseeable misuse of devices. Consideration of foreseeable misuse through cyber security failures can include:

- Malicious and unauthorised access to or modification of a device
- Exploitation of known vulnerabilities in the device software
- Unsupported user modification of devices to customise a device to perceived needs or preferences
- Use of device in operating environments that are not or may not be secure
- Results of off-label use of devices by clinicians in certain situations

Examples of cyber security considerations for manufacturers and sponsors as they relate to a number of the Essential Principles are highlighted in Table 1.

Table 1: The Essential Principles and cyber security considerations

Essential Principle	Cyber security considerations
1. Use of medical devices not to compromise health and safety	• Is there risk that a cyber security vulnerability may lead to the medical device compromising the health and safety of the user? • Is that risk acceptable? • What is the intended cyber exposure? • Is there risk that the device could compromise the safety and health of other people (e.g. could the device compromise a network with other connected medical devices?)

[2] See Division 1 of Part 4-11 of Chapter 4 of the *Therapeutic Goods Act 1989*.

Essential Principle	Cyber security considerations
2. Design and construction of medical devices to conform to safety principles	• Has cyber security been considered in the design of the medical device? Have principles of inherently safe design (e.g. secure by design; quality by design) been used to reduce cyber security risks to patient safety? • What is the generally acknowledged state of the art for cyber security for this type of product and does product development meet this? • Has a risk assessment been conducted to identify cyber security related risks associated with use and foreseeable misuse of the device and has consideration been given to eliminating or minimising these risks? • If appropriate, does the device have the capability to log cyber security issues or raise an alarm if at risk? • Has cyber security been considered across the total product lifecycle of the device? • What is the usability of the cyber security functionality within the device? Is there risk associated with applying security updates?
3. Medical devices to be suitable for intended purpose	• Has consideration been given to the conditions under which the device is intended to be connected? Are there known cyber security vulnerabilities or risks that can impact the intended performance of the device? For example, is a communication protocol or third party component used by the device known to be vulnerable to certain attacks?
4. Long-term safety	• Is the cyber security of the device able to be regularly maintained? Is it "patchable" and/or updatable? How will updates be delivered and are accessories required? • What are the relevant end-of-life procedures for the device?
5. Medical devices not to be adversely affected by transport or storage	• Can a device be compromised through its supply chain and transport system? Can cyber security vulnerabilities be introduced? Are there methods available to detect any compromise? • Does the user need to take any actions to update the device following a period of storage? Are these instructions clear?
6. Benefit of medical devices to outweigh any undesirable effects	• Does the benefit of the device outweigh the cyber security (and other) risks associated with the use of the device? • Do any new features that may increase cyber security risk also have an increased benefit?

Essential Principle	Cyber security considerations
9. Construction and environmental properties	• If the medical device is intended to be used in combination with other devices, equipment or accessories, has consideration been given to how the intended performance of the medical device might be impacted by cyber threats in other devices or other networks? • What are the cyber threats from other devices or equipment and are there any new cyber threats in the combination? How can these threats be mitigated? • Are there environmental conditions that need to be considered to minimise the risks associated with the use of the medical device (e.g. known vulnerabilities and exploits)? What are the essential environmental security controls, e.g., isolation, firewalling, intrusion detection systems, etc.? • How has cyber security maintenance been considered? Is this maintenance practicable during use of the device on the market? Is the security embedded within the device usable for end-users, and will lack of maintenance cause unacceptable risks?
10. Medical devices with a measuring function	• Could a cyber exploit affect the measurement accuracy, precision and stability of the medical device? Is the integrity of the data vulnerable to cyber-attacks? • If measurements become inaccurate, could this result in harm to a patient?
12. Medical devices connected to or equipped with an energy source	• Can the performance, reliability, and repeatability of the device be impacted by cyber threats? • Are there alarm systems to indicate a power failure or warn the user of possible patient harm? Can the integrity of these alarms be altered by adversaries? Is there an appropriate system alarm in place for known vulnerabilities? • If a medical device administers energy or substances, has consideration been given to protecting the device from cyber security threats that could cause the device to withhold or deliver too much energy/substance? • If appropriate, does the device have the capability to log cyber security issues? • Are there unique cyber security conditions that need to be considered for active implantable medical devices, especially with regards to programing interfaces?

Essential Principle	Cyber security considerations
13. Information to be provided with medical devices	• Does the information provided with the device explain how to use the device safely with regards to minimising potential cyber security implications? • What security is recommended / required for networks that this device connects to? • Does the information explain to users how to maintain cyber security for the device, and the steps to take during and after a cyber incident? Is there risk associated with applying security updates? • Is providing cyber security information and instructions for maintenance and use adequate to explain how to use the device safely, or does the user require education as well? • How will cyber security information be provided to software products and accessories?

Relevant standards

As indicated in Part 1, Essential Principles, the application of standards is one way to ensure medical devices are compliant with the Essential Principles, although their use is not mandated by the TGA. Medical devices that have cyber security risk/s are highly variable in their components and operate in a variety of environments, resulting in many relevant standards. The matrix below (Table 2) presents a summary of standards recognised as being desirable to meet regulatory requirements for cyber security of medical devices, alongside the relevant Essential Principle that may be demonstrated.

As technology evolves and new standards are developed, manufacturers and sponsors will need to be aware of the changing state of the art relevant to their devices.

Table 2: Standards recognised as desirable to meet regulatory requirements for cyber security of medical devices, alongside the relevant Essential Principles.

Standard	Scope	EP1	EP2	EP3	EP4	EP5	EP6	EP9	EP10	EP12	EP13
ISO 14971 Medical devices - Application of risk management to medical devices	A process for a manufacturer to identify the hazards associated with medical devices, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls.	✓	✓	✓	✓		✓	✓		✓	
ISO 13485 Medical device – Quality management systems	Specifies requirements for QMS where an organisation needs to demonstrate its ability to provide medical devices and related services that consistently meet customer and applicable regulatory requirements.	✓	✓	✓	✓	✓			✓		
IEC/EN 62304 Medical device – Software lifecycle requirements	Defines the life cycle requirements for medical device software: the set of processes, activities, and tasks including development, maintenance, configuration management and problem resolution.		✓		✓	✓	✓	✓			✓
IEC 60601-1 Safety and essential performance of medical electrical equipment	Widely accepted benchmark for medical electrical equipment. The standard covers safety and performance for electrical medical devices and specifies safety requirements including those for electrical, mechanical, and thermal hazards, as well as some requirements for Programmable Electrical Medical Systems (PEMS) – the use of software.		✓			✓		✓	✓	✓	

Standard	Scope	EP1	EP2	EP3	EP4	EP5	EP6	EP9	EP10	EP12	EP13
UL 2900-1 Software Cybersecurity for Network-Connectable Products	Applies to network-connectable products that shall be evaluated and tested for vulnerabilities, software weaknesses and malware: (i) developer risk management process requirements; (ii) methods to test vulnerabilities, software weaknesses and malware; and (iii) security risk control requirements.	✓	✓	✓	✓			✓		✓	
UL 2900-2-1 Requirements for Network Connectable Components	Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems. It is a security evaluation standard that applies medical devices, accessories to medical devices and medical device data systems.	✓	✓	✓	✓			✓		✓	
IEC 80001 Application of risk management for IT-networks incorporating medical devices	80001 series of standards define roles, responsibilities and activities for risk management of IT-networks incorporating medical devices. Focus is on safety, effectiveness, data security and system security.	✓	✓	✓				✓			
AAMI/UL 2800 Safety and security requirements of interoperable medical systems	Defines safety specifications that a medical devices interface should be labelled in order to operate in safe conditions. Focuses on risks associated with interoperability within the integrated clinical environment.		✓	✓				✓		✓	✓

Standard	Scope	EP1	EP2	EP3	EP4	EP5	EP6	EP9	EP10	EP12	EP13
AAMI/TIR 57 Principles for medical device information security management	Methods to perform information security risk management for medical device within the context of ISO 14971. Incorporates the view of risk management from IEC 80001-1.	✓	✓	✓	✓		✓	✓		✓	
IEC 80002 Medical device software standards (series)	Provides guidance on the application of ISO 14971 to medical device software, methods for validation of software for medical device including any software used in device design, testing, component acceptance, manufacturing, labelling, packaging, distribution and complaint handling or to automate any other aspect of a medical device quality system.	✓	✓	✓	✓		✓	✓		✓	✓
ISO 15408 Evaluation criteria for IT security	Common criteria. Establishes general concepts and principles of IT security evaluation, models for evaluation of security properties of IT products.	✓	✓	✓	✓			✓		✓	
IEC 82304 Health software - general requirements for product safety	Covers entire lifecycle including design, development, validation, installation, maintenance, and disposal of health software products. Covers safety and security of health software products designed to operate on general computing platforms and intended to be placed on the market without dedicated hardware.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ISO/IEC 29147 Disclosure of potential vulnerabilities in products	Details the methods a vendor should use for the disclosure of potential vulnerabilities in products and online services.	✓			✓			✓			✓

Standard	Scope	EP1	EP2	EP3	EP4	EP5	EP6	EP9	EP10	EP12	EP13
ISO/IEC 30111 Resolve potential vulnerability information in a product	Explains how to process and resolve potential vulnerability information in a product or online service.	✓	✓	✓	✓	✓	✓	✓			✓
ISO/IEC 27000 series											
ISO 27799 Health informatics - Information security management in health using ISO/IEC 27002	Explains organisational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organisation's information security risk environment(s).				✓	✓		✓			✓
IEC 62366-1 Medical devices – Part 1: Application of usability engineering to medical devices	Specifies a process for a manufacturer to analyse, specify, develop and evaluate the usability of a medical device as it related to safety	✓	✓	✓	✓			✓		✓	✓
IEC/TR 62366-2 Medical devices – Part 2: Guidance on the application of usability engineering to medical devices	Contains background information and provides guidance that address specific areas that experience suggests can be helpful for those implementing a usability engineering (human factors engineering) process	✓	✓	✓	✓		✓	✓		✓	

Cyber security risk monitoring

To ensure that a medical device included in the ARTG continues to meet the requirements of the Essential Principles, a manufacturer or sponsor must demonstrate how they will gather information regarding emerging cyber security vulnerabilities that may impact the safe operation of their medical device and how these will be addressed. Manufacturers should also share information with the TGA, see section on post market, and the wider industry regarding cyber security vulnerabilities and threats that they discover, refer to Appendix 4.

Pre-market guidance

Regulatory requirements

Sponsors intending to include a medical device on the ARTG for supply in Australia need to meet their legal obligations under the Act and MD Regulations. In demonstrating compliance with the Essential Principle the Sponsor needs to demonstrate that cyber security risks have been minimised.

For all classes of medical devices, evidence is required to be made available when requested by the TGA to demonstrate that medical device cyber security risk is being managed by appropriate quality management systems and risk management frameworks. The regulations specify that some applications are subject to mandatory application audits, with other types of applications subject to non-mandatory application audits.

All medical devices that include software are susceptible to cyber security risks. Manufacturers of medical devices must have a quality management system that demonstrates how cyber security risk has been minimised during the design, development, manufacturing, and supply of a medical device, and how post-market requirements will be satisfied. This is critical to reduce the probability of a cyber security vulnerability being exploited to create a threat, leading to unacceptable risk to a patient, and for the management of emerging and ongoing cyber security risk.

Development approach

To meet the requirements of the relevant Essential Principles, a manufacturer is required to eliminate identified cyber security risk, or reduce the risk to an acceptable level. Sponsors must also consider the potential for new cyber security threats that will emerge over the usable life of the device, planning for upgrade pathways to address these issues once the device is on the market, and planning for device obsolescence.

To reduce cyber security risk throughout the design and development phases, there are two approaches that assist in understanding cyber security risk as early as possible. Consideration of these approaches also assists with compliance with the Essential Principles. They include:

- Develop an understanding of cyber security vulnerabilities associated with the medical device, and the potential risk, during the initial design and development phase. Early assessment allows adaptable cyber security measures to be incorporated in the device design (this is generally called secure-by-design).

- Understand the potential cyber security risk associated with each function of the medical device. While an increase in functions (e.g. Bluetooth connectivity) may lead to improved usability, it also increases the device exposure to cyber security vulnerabilities. More exposure increases the probability of a cyber security vulnerability being exploited, leading to potentially unacceptable risk. Early assessment allows for a stronger balance between functionality and cyber security (this is generally called quality-by-design).

Application of standards

In order to meet the Essential Principles, there is an expectation from the TGA that medical device manufacturers will have "regard to the generally acknowledged state of the art"[3]. In many instances, this expectation is readily achieved by the application of existing standards, which are outlined in Part 1, Relevant Standards. The standards in Table 3 are expected as a baseline during the design and development of a medical device; however, depending on the device, compliance with the Essential Principles may necessitate implementation of additional standards (information in Part 1, Relevant Standards).

Table 3: Key standards for consideration

Standard	Scope
ISO 14971	Medical devices - Application of risk management to medical devices
ISO 13485	Medical devices - Quality management systems
IEC/EN 62304	Medical devices - Software lifecycle requirements
IEC 60601-1	Safety and essential performance of medical electrical equipment

Risk management strategies

The development of risk management strategies – the continuous approach to identifying, estimating and reducing risk – is required in order for a medical device to comply with the Essential Principles; cyber security risk management can be readily included in these strategies.

National Institute of Standards and Technology

Development of a risk management strategy in line with the USA's National Institute of Standards and Technology's (NIST) cyber security framework is a globally accepted approach by the cyber security community as a way to address cyber security risks throughout the life cycle of a (medical) device. The framework describes a series of concurrent and continuous cyber security functions that underpin a cyber security risk management strategy[4]:

- **Identify**: Develop an organisational understanding of cyber security to effectively manage cyber security risk associated with medical devices
- **Protect**: Develop and implement appropriate actions to ensure that a medical device can safely deliver its intended function, balancing security and usability
- **Detect**: Develop and implement appropriate activities to identify the occurrence of a cyber security event that changes the risk profile of a medical device
- **Respond**: Take appropriate action to ensure that cyber security risk is minimised for a medical device with a new risk profile

[3] *Therapeutic Goods (Medical Devices) Regulations 2002*, Schedule 1, clause 2(1) – Essential Principle 2(1)

[4] NIST (2018). *Framework for Improving Critical Infrastructure Cybersecurity*, [Online] Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Accessed: 28/09/2018

- **Recover**: Implement activities to increase medical device cyber resilience and to restore any capabilities or services that were impaired due to a cyber security incident

Implementing a cyber security risk management strategy that is based on this framework may assist in meeting the requirement for a medical device to obtain and maintain regulatory compliance in Australia.

International Standards Organisation

ISO 14971 details the process that a manufacturer can take in order to complete risk identification, risk evaluation, and implementation of risk control measures, that if correctly implemented will meet regulatory requirements. The following summary is an example of a risk management process under ISO 14971[5]:

1. **Implement a risk management framework**
   a. Establish the risk management process
   b. Establish relevant roles and responsibilities
   c. Establish appropriate documentation
   d. Create a version controlled risk management file
2. **Define the intended use of the medical device**
3. **Identify hazards**
   a. What are the known cyber security vulnerabilities?
4. **Define hazardous situations and foreseeable use**
   a. Develop cyber security scenarios that are likely in the foreseeable use
5. **Estimate the level of risk**
   a. How likely is it that cyber security vulnerabilities will be exploited to create unacceptable levels of risk?
6. **Evaluate the identified risk**
   a. Is the risk acceptable?
   b. If not acceptable, it will need to be eliminated or reduced to an acceptable level
7. **Risk control**
   a. Has the cyber security risk been reduced to a level that is outweighed by the benefits of the component/function that introduced the risk?
8. **Evaluate entire product risk acceptability**
   a. Is the risk acceptable?
   b. Do the benefits of the medical device outweigh the risks?

[5] Speer, J. (n.d.). *The definitive guide to ISO 14971 risk management for medical devices*, [Online] Available from: https://www.greenlight.guru/hubfs/Sales_Material/gg_guide_to_risk_management.pdf. Accessed: 9/11/2018

9. **Risk management reporting**
   a. Complete a review and prepare appropriate documentation and reports prior to seeking regulatory approval.
10. **Post-market risk management**
   a. Complete activities for risk minimisation from a total product life cycle perspective; internal risk management audits, corrective and preventative action (CAPAs), etc.

Supply chain assessment

Medical device manufacturers need to consider the cyber security practices of their supply chain, ensuring that components (including software) used within or for the construction of the device are appropriately cyber secure, and will meet the requirements of the Essential Principles (in particular Essential Principles 2[6], 4[7], 5[8], and 9[9]).

Contractual negotiations and agreements should clearly outline cyber security expectations from the medical device manufacturer or sponsor responsible for the device once it is supplied in Australia. Manufacturers should investigate and ask questions to understand the cyber security practices of their suppliers, as well as their response plans following breaches or discovery of vulnerabilities. Agreements should include expectations about cyber security practices of third parties to ensure the confidentiality, integrity and availability of applicable systems

Provision of information for users

Essential Principle 9 requires, among other things, that a medical device manufacturer to ensure that a medical device is designed and produced in a way that ensures that, as far as practicable, the risks associated with reasonably foreseeable environmental conditions are removed or minimised[10]. To meet this requirement and those of Essential Principle 13[11], appropriate technical and plain-language information should be provided to users of medical devices, and this should be considerate of the level of cyber security education that the intended user has received.

Clinicians should be armed with the information they need to have a meaningful discussion with the patient about the risks and benefits of the device, including cyber security risk. They should also have access to information to decide whether a particular security patch should be applied or not.

Provision of information is also important for consumer focused SaMD products, where the device may be used in a home environment (with limited cyber security protection) or a public environment which by nature is highly accessible.

[6] Essential Principle 2 (Design and construction of medical devices to conform with safety principles)
[7] Essential Principle 4 (Long-term safety)
[8] Essential Principle 5 (Medical devices not to be adversely affected by transport or storage)
[9] Essential Principle 9 (Construction and environmental properties)
[10] Essential Principle 9.2(b)
[11] Essential Principle 13 (Information to be provided with medical device)

Technical considerations

Cyber security performance testing

- Consider implementing penetration testing initiatives to validate the effectiveness of medical device cyber security measures, and internal risk management practices:
  - Invasive tests involving simulated malicious attacks to evaluate the effectiveness of managing possible and probable attacks, e.g. malicious input, authentication bypass, and illicit operation.
  - Collaboration with “white-hat” adversaries, biomedical engineering teams and cyber security professionals via conferences, formal and informal networks.
  - It is recognised that some critical systems may not be removed from production for testing, and if feasible, a twin system for testing is recommended to overcome this.
- Performance testing should cover assessment of common cyber security vulnerabilities (examples in Appendix 6) through database checks, use of known exploits and tools (e.g. Kali Linux with Metasploit) or software behaviour analysis using specific scenarios, including:
  - Use of insecure function calls, e.g. causing overflow type of vulnerabilities
  - Insufficient protection for security credentials, e.g. hard-coded passwords
  - Insufficient information security capabilities, e.g. missing or improper use of confidentiality, integrity and availability measures
  - (Un)intentionally left debugging features and comments, e.g. debugging hooks
  - Improper use of control statements, e.g. improper checks for unusual or exceptional conditions
  - Wrong implementation of algorithms and protocols, e.g. OpenSSL Heartbleed
  - Flaws in algorithm and protocol designs, e.g. Compression Ratio Info-leak Made Easy (CRIME) vulnerability of TLS Compression
  - Malicious codes and code segments, e.g. malwares such as virus and worms
  - Software components development through an unknown or incompetent development process, i.e. software of unknown provenance (SOUP)
  - Listed (e.g. NVD, CERT, ACSC) vulnerabilities for off-the-shelf components (kernel, driver, firmware, application), libraries and API
  - Lack of input sanitation and data validation, e.g. allowing potential injection attacks.
- Take action on outcomes by assessing the risk vs. benefit of impacted functions, and consider solutions that reduce the risk.

Modularised design architecture

- It is best practice to, modularise or partition aspects of the design architecture to enable independent function of modules when one is attacked, reducing the impact of a cyber security attack by containment.
- A modularised approach promotes medical devices that can be updated and adapted to changes in the cyber security risk profile over the total life cycle of the product.

- Smaller components are easier to assess for cyber resilience, by application of methods including mathematical formal proofs, e.g. security verified micro kernels. Reuse of validated or verified modules in different devices will improve overall cyber security, with reduced effort.

Operating platform security

- Assessment of the cyber security (under the development approach) of third party operating systems and hardware platforms needs to be completed in order to meet the Essential Principles, in particular Essential Principles 2[12], 3[13] and 9[14].
- This is particularly critical for SaMD development where the product is intended to operate on a consumer mobile device:
  - It is required that the manufacturer or sponsor will have assessed the cyber security risks introduced by the mobile hardware and operating system in order to meet the Essential Principles.
- High-level considerations include the cyber security protections and support that a third party provides for its platform, the ability to remove or disable unused functions, its default network security, and its accessibility if the user is expected to complete patching and performance updates.
- When possible, reduce the number and complexity of operating system components to reduce the attack surface, e.g. by using a simplified kernel design, or a stripped down operating system.
- When possible, implement code signing for firmware updates. These signatures include a signed hash of the firmware code which can be checked by the device before installing. An incorrect signature indicates that the firmware is from an unauthorised (malicious) source or the firmware code has been tampered with.

Emerging software

- Emerging software technologies should be considered against Essential Principle 2 (design and construction of medical devices to confirm with safety principles), and managed under standards such as ISO 14971, with continued monitoring of state of the art for cyber security risk minimisation in aligned jurisdictions and industries.
  - For example, medical devices that incorporate artificial intelligence (AI) or use machine learning (ML) software components are required to demonstrate that these components have been integrated in such a way that cyber security risk has been minimised, and that foreseeable changes in software have been considered.
- It is recognised that some standards, e.g. ISO/IEC 15408 Common Criteria, cannot readily accommodate the evolving nature of AI code or the changing outcomes from ML algorithms.

Update pathways

- Manufacturers must consider the ability for secure updating of a medical device during its lifecycle of the device to account for emerging cyber risks, and demonstrate the approach is in alignment with current state of the art practice.

[12] Essential Principle 2 (Design and construction of medical devices to confirm with safety principles)

[13] Essential Principle 3 (Medical devices to be suitable for intended purpose)

[14] Essential Principle 9 (Construction and environmental properties)

  - Cyber security risk that update methods may introduce must be considered, for example, remote access and continuous deployment systems that use cloud/virtual systems are efficient modes for updates, but will introduce risks.

Trusted access and content provision

- Manufacturers and sponsors are encouraged to implement trusted access measures for network connected devices to prevent unnecessary cyber security risk. This should focus on securing activities that will be undertaken by the medical device user, including reasonable access to the device (i.e. balancing access and security), and its own access to networks beyond what is absolutely necessary, for example:
  - Remove internet accessibility and direct network connectivity
  - Incorporate multi-factor authentication
  - User profiles that limit device access and device privileges.

Post-market guidance

Regulatory requirements

> The TGA will always assess compliance with the Essential Principles against the current risk environment, regardless of which risks existed when the device was included in the ARTG. Evidence of compliance with the Essential Principles, and other legislation, must be supplied to the TGA if requested.

The inclusion of a kind of medical device on the ARTG is subject to certain statutory conditions which include, for example, an obligation to maintain sufficient information to substantiate compliance with the Essential Principles or have procedures in place with the manufacturer to ensure such information can be obtained[15]. Breaching the conditions of the inclusion of a kind of medical device may lead to suspension or cancellation of the entry for that device from the ARTG[16], may be an offence[17], and may contravene a civil penalty provision[18].

Consistently with these legislative requirements and in line with a total product life cycle (TPLC) strategy, once a medical device has been included on the ARTG, it must continue to meet the requirements of the Essential Principles to remain on the ARTG. Risk management and quality management systems must be updated appropriately to maintain inclusion on the ARTG, and it is critical that the change management process, e.g. as outlined in IEC/EN 62304 standard, is documented to clearly outline how risk and quality management systems have been modified as the risk profile of the medical device evolves.

[15] See subsection 41FN(3) of the *Therapeutic Goods Act 1989*

[16] See Part 4-6 of Chapter 4 of the *Therapeutic Goods Act 1989*

[17] See subsections 41MN(1), (4) and (4A)) of the *Therapeutic Goods Act 1989*

[18] See subsection 41MNA(1)) of the *Therapeutic Goods Act 1989*

Therapeutic Goods Act 1989—Chapter 4, Part 4-5, Division 2, section 41FN(3)

41FN Conditions applying automatically

(3) The inclusion of a kind of medical device in the Register is subject to conditions that:

a. at all times while the inclusion in the Register has effect, the person in relation to whom the kind of device is included in the Register:

   i. has available sufficient information to substantiate compliance with the Essential Principles; or

   ii. has procedures in place, including a written agreement with the manufacturer of the kind of devices setting out the matters required by the regulations, to ensure that such information can be obtained from the manufacturer within the period specified in the regulations; and

b. at all times while the inclusion in the Register has effect, the person in relation to whom the kind of device is included in the Register:

   i. has available sufficient information to substantiate that the conformity assessment procedures have been applied to the kind of medical device or that requirements, comparable to those procedures, have been applied to the kind of medical device to the satisfaction of an overseas regulator; or

   ii. has available information relating to changes to the kind of medical device, the product range, and quality management system, of the manufacturer of the device; or

   iii. has procedures in place, including a written agreement with the manufacturer of the kind of devices setting out the matters required by the regulations, to ensure that such information can be obtained from the manufacturer within the period specified in the regulations; and

c. at any time while the inclusion in the Register has effect, the person in relation to whom the kind of device is included in the Register will, if asked to do so by the Secretary, give the information to the Secretary; and

d. the person in relation to whom the kind of device is included in the Register will give information of a kind mentioned in subsection 41MP(2) or 41MPA(2) to the Secretary within the period specified in the regulations; and

e. the person in relation to whom the kind of device is included in the Register will give the manufacturer of the kind of medical device information relevant to:

   i. the manufacturer's obligations under the conformity assessment procedures or requirements comparable to those procedures; and

   ii. whether medical devices of that kind comply with the Essential Principles.

Cyber security risk

Cyber security risk must be considered as part of the post-market risk management process. As with other risks, the changing nature of cyber security risks means that it cannot be mitigated through pre-market controls alone, and requires ongoing management. This leads to cyber security risk monitoring and management being an extension of the activities already conducted by a manufacturer and sponsor.

As with other risks, it is important for medical device manufacturers and sponsors to develop an understanding of how to assess cyber security risk. To do this effectively it is important to build a robust understanding of the relationship between cyber security vulnerabilities, exploits, and threats. This will assist a manufacturer or sponsor in understanding which course of action is required in response to the changed medical device cyber security risk profile, i.e. a device recall, safety alert, routine update or an adverse event report to the TGA. Figure 1 details the relationship between vulnerabilities, exploits, threats and risk, and the people who have adversary capabilities, commonly known as white hat and black hat.

Alongside white hat hackers and black hat adversaries, users of medical devices can unwittingly introduce cyber security risk themselves by attempting to make unauthorised modifications to enhance the device for their perceived needs. In some cases, these modifications may even be unintentional.

Vulnerabilities

Vulnerabilities are weakness in computer software code, hardware designs, information systems, security procedures, internal controls, or human behaviour that could be exploited by a threat.

Vulnerabilities are typically made known to the public once a verified patch exists; this can be via active cyber security monitoring (Part 1 Cyber security risk monitoring) or by notification to the manufacturer/sponsor by a third party. When a vulnerability is published or discovered (like those detailed in Appendix 6), a manufacturer must assess the risk posed on the safe use of the medical device, and decide if corrective and preventative action (CAPA) is required based on the level of risk. Even if the risk is assessed to be acceptable due to a low probability of exploitation of the vulnerability, and the potential risk of harm to patients is negligible, the response should be documented as part of continuous risk management.

Essential Principle 2 requires that manufacturers eliminate or reduce risk as far as possible and inform users of the residual risk that arises from any shortcoming of the protection measures adopted.

Many vulnerabilities remain intentionally undisclosed, and may be leveraged by adversaries to create a "zero day" situation, namely when a publicly unknown vulnerability is used to create a cyber-attack ("zero day" reflects that the day of the attack and the disclosure of the vulnerability are the same). Even when meeting pre-market requirements for cyber security risk minimisation, vulnerabilities that impact a medical device can still be discovered and exploited.

Exploits

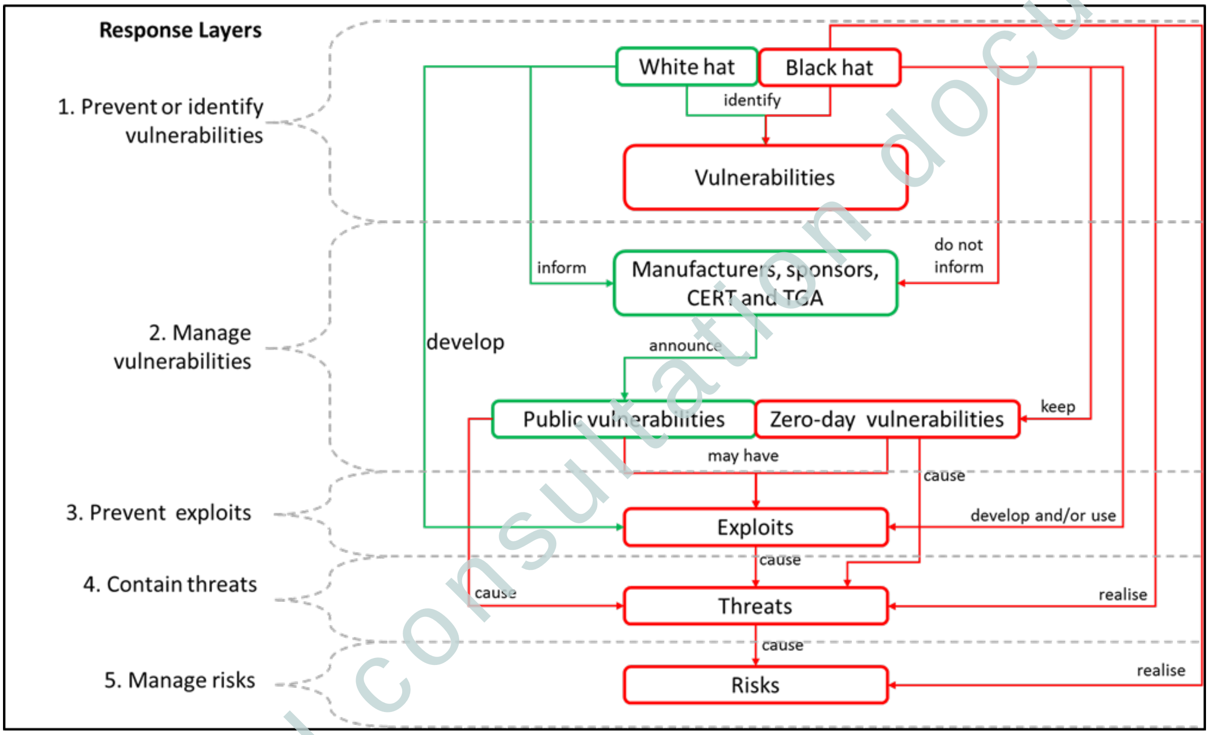
Vulnerabilities may have exploits - tools developed to take advantage of (one or more) vulnerabilities. Numerous exploits are publicly accessible, and are packaged as executables or source code. These exploits may also be packaged into toolsets for improved usability (e.g.

Metasploit and Kali Linux). Others exploits are not public, and are implemented to demonstrate that the vulnerabilities can be used to compromise an ecosystem.

Threats

Black hat adversaries may instigate an attack, which can cause cyber security threats. For example, the threat that patient data is exposed to unauthorised individuals, or that the operation of a device is compromised such that it can no longer complete its intended task, impacting the safety of the patient. A single threat might strategically use several exploits to achieve the adversary's final objective. The existence of threats on medical devices leads to risks, and manufactures and sponsors must respond to minimise the risks, as outlined in the following section.

Figure 1: Vulnerabilities, Exploits, Threats, Risks and Adversaries



Threat and risk response

To remain compliant with the Essential Principles a manufacturer or sponsor must establish, document, and update quality management and risk management systems throughout the lifecycle of a medical device. Documenting the effectiveness of any corrective of recall action is required as part of this process.

This involves an ongoing process for identifying hazards associated with the safe use of the medical device, including cyber security vulnerabilities, threats, and estimating and evaluating the associated risks, controlling these risks, and taking corrective action where necessary.

Monitoring issues

In alignment with a TPLC strategy, the approach to monitoring cyber security information should be clearly outlined during the development of the medical device. The outcome of all cyber security monitoring must be documented as part of ongoing risk management, regardless of the level of risk that the activity identifies. Cyber security vulnerabilities, threats and risks may be identified by numerous different parties along the supply chain, including:

- The manufacturer (through an effective quality management system)
- The Australian sponsor (through adverse event reports, complaints, and monitoring of CERT alerts)
- TGA (through post-market monitoring and compliance activities)
- Other regulators, who may notify TGA
- White hat hackers and researchers, who may notify the TGA, sponsor or manufacturer
- Users, including patients and consumers, health service providers, and administrators
- Third party audits (e.g. by clients), inspections by other regulators and other avenues
- Media (traditional and social).

Cyber threat information sharing is an important component for a safe and secure digital ecosystem. Such an information system provides all parties along the supply chain, but especially the manufacturer and sponsor, with the capability to identify threats and assess associated risks. Information empowers organisations with knowledge to monitor threats and respond accordingly.

In Australia, options for organisations to formally share information on cyber security threats are currently limited; however, the TGA encourages informal networks to share information. Some modes for sharing threat information in Australia are outlined in Part 1 Regulatory requirements.

Risk assessment

A manufacturer and/or sponsor's assessment of the risk of patient harm posed by a cyber security hazard that impacts the safety, quality, performance or presentation of a device should consider:

- The exploitability of the cyber security vulnerability/threat
  - Estimating the likelihood of a cyber security exploit is difficult. Manufacturers/sponsors should consider using a cyber security vulnerability assessment tool or similar scoring system for rating vulnerabilities and determining the need for and urgency of the response. An example is the Common Vulnerability Scoring System (CVSS). Many factors are important to consider here, including ability to detect the vulnerability.
- The severity of patient harm (physical and psychological) if the vulnerability were to be exploited (Figure 1)[19]

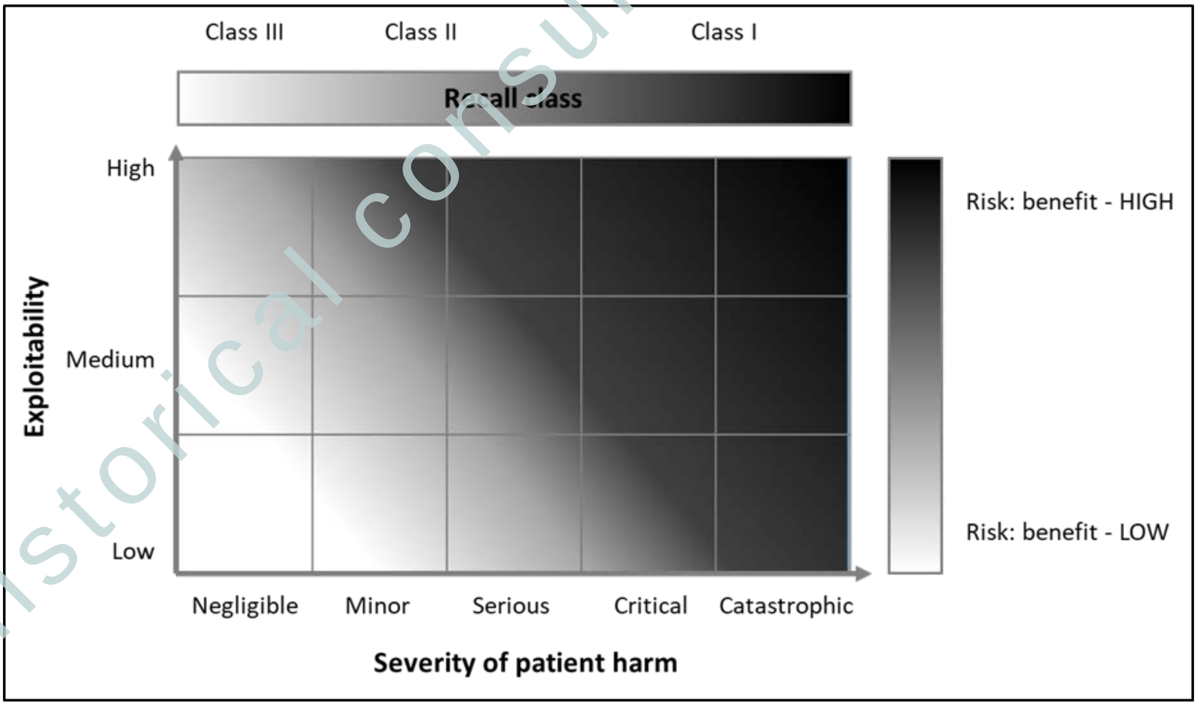
[19] As noted above, potential harm to a patient from the exploitation of a cyber security vulnerability may include physical or psychological harm through negative impact on the patient's health and safety. Other risks may be privacy or financial.

- Manufacturers/sponsors should have a process for assessing the severity of patient harm should the cyber security vulnerability be exploited. One approach is based on qualitative severity levels as described in ISO 14971:2007.
  - **Negligible**: Inconvenience or temporary discomfort
  - **Minor**: Results in temporary injury or impairment not requiring professional medical intervention
  - **Serious**: Results in injury or impairment requiring professional medical intervention
  - **Critical**: Results in permanent impairment or life-threatening injury or injury to many patients
  - **Catastrophic**: Results in patient death, or permanent impairment to many patients

By considering these, manufacturers/sponsors can evaluate whether cyber security vulnerability is creating potential risks associated with an adverse event, a medical device failure or a complaint, and understand if the risk of patient harm is acceptable or unacceptable.

Independent of the outcome of a risk assessment, it is required that all risk assessment activities (including the cyber security monitoring activities outlined above) will be captured, demonstrating application of the risk management strategy (e.g. application of ISO14971) outlined as part of the pre-market activities. This must include corrective and preventative action (CAPA) plans and incident response activities. Quality management systems should also be updated, if applicable.

Figure 2: Evaluation of Risk of Patient Harm



Modified from the FDA post-market guidance on cyber security for medical devices

Manufacturers are required to remediate cyber security vulnerabilities to reduce the risk of patient harm to an acceptable level.

- Where risk of patient harm is acceptable, sponsors and manufacturers are required to proactively promote practices that continue to reduce cyber security risks even when residual risk is acceptable. In such circumstances, consideration could be given to initiating non-recall action if the medical device meets all specifications/standards and no deficiencies exist in safety, quality, performance or presentation.
- Where a medical device is identified as being defective and/or the risk of patient harm is unacceptable, sponsors (along with the relevant manufacturer) must take appropriate actions (agreed with TGA) to remediate risks to public health and safety, as effectively as possible through a type of recall action. This includes sharing of relevant information with sponsors, regulators, customers and the wider user community, and implementing compensating controls to adequately mitigate the risk. Reporting requirements must also be acted on.

Immediate recalls

Cyber security vulnerabilities, threats and risks may be discovered that pose an **immediate and significant threat to the health and safety of users**. These cyber security issues may also indicate that there has been actual or potential product tampering. These devices may require an immediate recall. If such a threat is found, sponsors must:

- Consult the Uniform Recall Procedure for Therapeutic Goods (URPTG) and follow this procedure as applicable; and
- Immediately contact the Australian Recall Coordinator.

Recalls (other than immediate recall)

Cyber security vulnerabilities, threats and risks may be discovered that result in **deficiencies or potential deficiencies to the safety, quality, performance or presentation** of a medical device and require appropriate recall action to ensure the health and safety of users.

If such a deficiency is found, sponsors must consult the URPTG, contact the Australian Recall Coordinator and follow the applicable parts of the procedure that apply to the situation at hand, in consultation with the TGA.

The URPTG defines four types of recall actions:

- **Recall** – action to remove a therapeutic good permanently from the market or from use
  - This action may be appropriate for high risk vulnerabilities to medical devices that are not able to be fixed in the field, or for those where a solution is not expected to be available within a suitable timeframe.
- **Product defect correction** – action undertaken to correct a specific or potential deficiency, including repair, modification, adjustment or re-labelling for reasons relating to deficiencies in quality, safety, performance or presentation. A product defect correction may also include updates or changes to any accessories, operating instructions or software.
  - This action may be appropriate for vulnerabilities to medical devices that are able to be corrected in the field and within a suitable timeframe.
- **Hazard alert** – an alert issued for an implanted therapeutic good that cannot be recalled.

- **Product defect alert** – an alert issued to raise awareness about concerns where discontinuation of treatment may be riskier than continued use of the deficient product (e.g. where no alternative product is available or recall would result in interruption of treatment).
  – This action may be suitable for vulnerabilities that cannot yet be fixed but where the risk of allowing the defective product to remain in use is deemed acceptable if managed appropriately.

The type of recall action for cyber security risks depends on the evaluation of the risk of patient harm, the nature of the deficiency and class of the recall. These need to be assessed on a case by case basis.

Figure 2 highlights the application of the TGA's three recall classes to the evaluation of patient harm. These include:

- **Class I: Most serious safety-related** – A situation where there is a reasonable probability that the use of, or exposure to, the deficient medical device will cause serious adverse health consequences or death. For example:
  – Software defects resulting in linear accelerators delivering the wrong radiation dose or delivering doses to the wrong location.
  – Hardware or software failures in ventilators resulting in shut down during use.
- **Class II: Urgent safety-related** – A situation in which use of, or exposure to, the deficient medical device may cause temporary or medically reversible adverse health consequences, or where the probability of serious adverse health consequences is remote. For example:
  – Infusion pumps giving visual or audible alarms due to software or hardware issues resulting in delay in infusion.
- **Class III: Lowest risk** – A situation in which use of, or exposure to, the deficient medical device is not likely to cause adverse health consequences.

Non-recall actions

Not all issues require recall actions. A non-recall action can be conducted if:

- The medical devices meet all specifications and standards, and
- There are no deficiencies in safety, quality, performance or presentation.

The decision to go ahead with a non-recall action needs to be made and agreed upon in consultation with the TGA.

Four types of non-recall actions may be appropriate:

- **Safety alert** – issued to provide information on the safe use of medical devices in certain situations where, although meeting all specifications and performance requirements, its use could present an unreasonable risk of harm if certain specified precautions are not followed.
  – This non-recall action may be appropriate if cyber security vulnerabilities to commonly used accessories, or networks that the device uses, becomes known.
- **Product notification** – issued to provide information about a medical device in a situation that is unlikely to involve significant adverse health consequences.
  – This non-recall action may be appropriate if a vulnerability poses a risk to data systems and privacy, but is unlikely to have adverse consequences on a user's health.

- **Quarantine** – suspension of future supply pending investigation of an issue or incident.
  - This non-recall action may be appropriate if it is suspected that a cyber vulnerability has caused an issue, but it is not yet confirmed.
- **Product withdrawal** – used to withdraw products for reasons that are not related to safety, quality, performance or presentation.
  - This non-recall action may be appropriate for removing vulnerable devices that are no longer supported by the manufacturer or devices that may become vulnerable due to withdrawal of support for third party components.

For more information on non-recall actions, consult the URPTG and follow as applicable.

Routine updates

Routine updates to device software are not uncommon. If these updates do not change the existing cyber security risk profile for the medical device, i.e. they are not responding to a known deficiency in safety, quality, performance or presentation, no recall action is required. Manufacturers and sponsors are required to update risk management systems based on the rollout of routine updates. However, are not required to notify TGA of routine software updates.

If sponsors or manufacturers are unclear as to whether a software update is 'routine' or whether it requires a type of recall or non-recall action, they should contact the Australian Recall Coordinator for advice in the first instance.

Other regulatory action

Alongside the recall and non-recall actions described above, the TGA has a range of other compliance tools it can use if risks identified in relation to a medical device are not managed appropriately. These include:[20]

- **Warnings and conditions** – the TGA may need to engage with manufacturers/sponsors and make them aware of its concerns about any non-compliance with regulatory obligations. TGA may also take other action that affects the Sponsor, including imposing conditions on the inclusion of the kind of device in the ARTG.
- **Suspensions and other enforcement action** – the identification of contraventions of the Therapeutic Goods Act and/or the MD Regulations may result in the TGA suspending the kind of medical device from the ARTG, or taking other regulatory action, such as accepting an enforceable undertaking or issuing an infringement notice to the Sponsor.
- **Cancellations and prosecution** – the entry of a kind of medical device may be cancelled from the ARTG in certain circumstances specified in the Act. Breaches of the Act or MD Regulations may also result in the TGA initiating civil or criminal proceedings. For example, civil penalties and also criminal offences apply under the Act for importing, supplying or exporting a medical device that does not comply with the Essential Principles.

[20] TGA (2013). *Regulatory compliance framework,* [Online] Available from: https://www.tga.gov.au/sites/default/files/compliance-framework.pdf. Accessed: 13/11/2018

Part 2 - Guidance for users

The TGA does not directly regulate all of the following supplementary considerations; however they are included for Users' reference; because they may have impact on the cyber security of medical devices.

This Section is structured with regards to major medical device users, as:

- Patients and consumers
- Small business operators
- Large scale service providers (inclusive of healthcare and medical professionals, and administrators and engineers)

Major medical device users include:

- **Patients and consumers** – who may use a medical device prescribed to them by a health professional, or alternatively may use a medical device (such as downloaded software "app") without professional supervision. Some consumers may access software that acts as a medical device (e.g. by diagnosing a heart murmur) from overseas websites, even though such software products may not have been evaluated or approved in Australia by the Therapeutic Goods Administration (TGA). The level cyber security in these software products can be highly variable.
- **Small business operators** – responsible for the procurement, implementation, maintenance, and application of medical devices in a small clinic environment or general medical practice. These users are generally reliant on manufacturer or sponsor information regarding medical device cyber security and may not have the ability to detect potential cyber security problems themselves.
- **Healthcare and medical professionals** – responsible for the use of medical devices for a range of purposes – described as "to diagnose, prevent, monitor, treat or alleviate disease or injury in a patient" in the *Therapeutic Goods Act 1989*. They are often based in a medium to large health or medical service environment such as public hospitals, private health service providers. These users may be able to access, review and exchange data with devices, and may also be responsible for patient education and establishing parameters for how devices and software are to be used. Healthcare and medical professionals include medical doctors, nurses, radiologists and radiographers, pathologists, etc.
- **Administrators and engineers** – responsible for the procurement, implementation and maintenance of medical devices in a health and medical service environment, such as a hospital. This includes biomedical engineers and IT experts who have the task of ensuring continuous operation of health services and generally have a high level of cyber security knowledge and expertise.

While supplying and maintaining a compliant medical device is the responsibility of the manufacturer and sponsor (usually the company making the device available on the Australian market), a compliant medical device will only be as secure as the most vulnerable aspect of the system it is expected to operate in. Users of medical devices also have share responsibility for providing a cyber secure environment for these devices to operate in.

TGA requires medical device manufacturers and sponsors to consider the foreseeable user environments for medical device software. Manufacturers and sponsors must also provide TGA with adequate information on how to safely use a medical device with cyber security risk.

However, operating environments are highly variable and cyber security risks are dependent on the knowledge and expertise and approach of those who use medical devices.

The following guidance aims to provide users with strategies that help to ensure a medical device is being used in an environment that minimises cyber security risks.

Patients and consumers

Patients and consumers using connected medical devices should take proactive action to protect their devices and networks, and act responsibly online. A consumer factsheet is included at Appendix 7.

The **Australian Government's Stay Smart Online** program provides guidance to consumers and small business operators to help reduce cyber security risk associated with software vulnerabilities, online scams, malicious activities, and online behaviours[21]. This guidance is important for creating a cyber safe operating environment for connected medical devices and assisting in maintaining the confidentiality, integrity and availability of medical device data. By doing so, it will assist in maintaining the operating integrity of a medical device so that it may continue to deliver a therapeutic benefit to the user of the product. Major aspects of the Stay Smart Online program for individuals[22] are highlighted below, together with consideration for the cyber safe use of medical devices.

Privacy

Home users should be aware of what content they share online, both in public and private forums, particularly relating to personal information.

- Some digital health products (e.g. Software as a Medical Device, such as medical software Apps) may provide a forum for users to interact. However, sharing of information that can lead to personal identification should be carefully considered.

Passphrases

Strong, hard-to-guess passphrases (a phrase rather than a word) and two-factor authentication where available, are recommended for network and account access.

- Many connected medical devices will require an account to be created, either in a companion app or an associated online platform. It is recommended that strong passphrases be used to protect these accounts, their associated information and any control that unauthorised access may allow.
- The US National Institute of Science and Technology (NIST) recommends that long and memorable passphrases (e.g. four or more common words) are more effective that a string of characters. However NIST recommends against changing passphrases periodically unless there is a user request or evidence of compromise[23].

[21] StaySmartOnline (n.d.). *About us*, : https://www.staysmartonline.gov.au/about-us

[22] StaySmartOnline (2016). *My Guide online security guide*, https://www.staysmartonline.gov.au/sites/g/files/net1886/f/Stay-Smart-Online-My-Guide.PDF

[23] NIST (2017). *NIST Special Publication 800-63B Digital Identity Guidelines*, https://pages.nist.gov/800-63-3/sp800-63b.html

Suspicious messaging

Treat any unexpected message with caution.

- Some devices, and even some treating healthcare and medical professionals, will communicate to a patient/consumer via electronic messaging (e.g. text message, email, chat function on web portal). Users should exercise caution and ensure that the message is trusted before acting on any information contained within it. If in doubt, contact the sponsor or medical professional, but use contact details listed in a place other than within the suspicious message.

Responsible browsing

Users should minimise visits to unknown websites and look for the padlock symbol and 'https' in the browser address when visiting sites. These indicate secure websites.

Online finances and payments

Criminals are eager to steal online banking details – users should keep computers up-to-date with anti-virus, anti-spyware and firewall software and use security measures recommended by the user's bank.

- Similar to online banking details, criminals are eager to steal personally identifiable health information. Users should ensure that connected devices - including computers, mobile devices, and medical devices - comply with the operating instructions provided with a medical device.

Tablets and mobiles

Users should turn on the security features of their mobile devices, set a password/phrase or PIN that must be entered to unlock the device, install reputable security software and ensure they are using the most up-to-date operating systems.

- These considerations are especially important when using a companion app for a connected medical device, or a Software as a Medical Device (SaMD) product, that may be completely operated and stored on a mobile device.

Backups and protection

Users should regularly update applications (including anti-virus software and plugins), firmware and operating systems to fix known vulnerabilities, and regularly back up data.

- Regularly updating applications associated with medical devices is important so that the most up-to-date software available is being used.
- If the medical device is used under the guidance of a medical professional, users should seek their advice with regards to updating software. Updating security software is important for continued protection of home based IT infrastructure on which many medical devices rely upon. Users should also regularly update the firmware within their routers.

Reporting

Help create a safer online environment by reporting potential cyber issues.

If a medical device appears to have been impacted by a cyber security issue and could directly impact health and safety, users should report this as soon as possible to their medical professional, and also directly to the TGA by phoning 1800 809 361.

Malicious cyber security activity can also be reported to is the Australian Cyber Security Centre (hotline on 1300 CYBER1 (1300 292 371).

The Stay Smart Online program also offers the following advice for users of smart devices in the home, which may include medical devices:

- Whenever possible, change any default passwords on the device to a secure and private passphrase.
- When practical, ensure software updates are set to apply automatically on any devices.
  - Special consideration should be given for medical devices: ensure that any updates provided for devices that may control or act as a connection point are compliant with the medical device – information concerning this should be available from the medical device sponsor.
- Follow all instructions when installing and configuring the settings for the device.
  - Patients and consumers using connected medical devices should always read and understand the information provided with the medical device, including its intended purpose and any limitations to use, the instructions for maintenance and use of the device, and how updates are to be provided for the device (e.g. software and firmware updates). Patients and consumers should also talk to their clinician if they have any questions about the instructions.
- Continue to be vigilant about protecting devices throughout their lifespan.

When using connected medical devices outside the home, users should exercise caution, especially if using public wireless networks or internet "hotspots" that are run by organisations that are not trusted, and avoid sending or receiving sensitive information while connected to public networks[24].

Small business operators

Small business operators have access to valuable data and information entrusted by patients, suppliers and employees, alongside access to medical devices that have been supplied to patients. The risks posed by inadequate medical device cyber security should be addressed as part of a business' plan for information management, including in relation to privacy.

The commencement of the Notifiable Data Breach scheme is an additional incentive for improved medical device cyber security. From February 2018, agencies and organisations

[24] StaySmartOnline (n.d.). *Using public wireless (or Wi-Fi) networks*, https://www.staysmartonline.gov.au/protect-yourself/doing-things-safely/using-public-wireless-or-wifi-networks

regulated under the *Privacy Act 1988 (Cth)* (Privacy Act) with personal information security obligations are required to notify affected individuals and the Office of the Australian Information Commissioner (when a data breach is likely to result in serious harm to individuals whose personal information is involved in the breach. Notifiable data breaches may give rise to complaints and other regulatory action under the Privacy Act[25].

Small businesses with significant involvement in medical device software should consider the guidance provided for large scale service providers, in particular development of an overarching risk management strategy, cyber secure procurement conditions, staff training, and cyber security planning.

Building on the advice provided for patients and consumers, the Australian Cyber Security Centre's Essential Eight Maturity Model aims to raise the cyber security resilience of Australian organisations. While no single risk mitigation strategy is guaranteed to prevent cyber security incidents, organisations are encouraged to implement all eight essential mitigation strategies as a baseline[26].

The Essential Eight

Mitigation strategies to prevent malware delivery and execution

1. **Application whitelisting** – to control the execution of unauthorised software
   - Approved/trusted programs are whitelisted to prevent execution of unapproved/malicious programs.
2. **Patching applications** – to remediate known security vulnerabilities
   - Patches for extreme risk security vulnerabilities in commonly used programs should be applied within 48 hours if possible. To help with this, when practical, and appropriate, organisations should ensure software updates are set to apply automatically.
3. **Configuring Microsoft Office macro settings** – to block untrusted macros
   - Microsoft Office macros can be used to deliver and execute malicious code on systems. Microsoft Office macros from the Internet should be blocked and settings should not be able to be changed by users.
4. **Application hardening** – to protect against vulnerable functionality
   - Flash, ads and Java are popular ways to deliver and execute malicious code on systems. These should be hardened – either blocked or set so that users cannot change settings.

Mitigation strategies to limit the extent of cyber security incidents

5. **Restricting administrative privileges** – to limit powerful access to systems
   - Admin accounts are the very powerful; adversaries can use these accounts to gain full access to information and systems. Requirements for these privileged accounts should be validated initially and on an annual or more frequent basis.

[25] See further the Office of the Australian Information Commissioner at www.oaic.gov.au

[26] Australian Cyber Security Centre (n.d.). *Essential Eight Maturity Model*, https://www.acsc.gov.au/publications/protect/Essential_Eight_Maturity_Model.pdf

6. **Patching operating systems** – to remediate known security vulnerabilities

   – Security vulnerabilities in operating systems can be used to further the compromise of systems. Verified patches for extreme cyber security risk within operating systems should be applied within 48 hours if possible, seeking clinical advice if required.

   – Medical device products that operate on systems that have received a patch in response to an extreme risk will need to be managed to ensure that they operate as expected on the patched system.

7. **Multi-factor authentication** – to protect against risky activities

   – Stronger user authentication makes it harder for adversaries to access sensitive information and systems. Multi-factor authentication should be implemented for all remote access users.

Mitigation strategies to recover data and system availability

8. **Daily backups** – to maintain the availability of critical data

   – This is important to ensure information can be accessed again following a cyber security incident. Backups should be tested in line with relevant medical information standards.

If a medical device appears to have been impacted by a cyber security issue, small business operators should directly report this to the TGA by phoning 1800 809 361.

Another avenue to report malicious cyber security activity is the Australian Cyber Security Centre hotline on 1300 CYBER1 (1300 292 371).

Large scale service providers

The following guidance[27] is applicable to Administrators and engineers and Healthcare and medical professionals.

It is aimed at users and organisations that are responsible for providing healthcare services to the population, typically in medium to large health and medical service environments. Some aspects are also applicable to small business operators. Continuous operation of health services can be readily disrupted by a successful cyber-attack, with cyber security vulnerabilities in a medical device being an accessible entry point for the attack.

Risk management strategy

Users responsible for implementing medical devices in critical health services should develop a clear and well documented risk management strategy. The primary goal is to develop an

[27] **Note**: The following guidance contains extracts, with the permission of the authors, from the document ‘Top Ten Strategies for Biomedical Device Security’, co-authored by James Fell, Department of Health and Human Services (Victoria) and Andrew Oldaker & Simon Cowley, The Royal Melbourne Hospital.

environment where risk to patients is minimised. The strategy will need to be revised as new types and classes of connected medical devices are added to the healthcare environment.

It is important that consideration is given to:

- Reducing the attack surface of the biomedical environment. This involves isolating networks from any untrusted network such as the internet, disabling any unused ports and services, only allowing real-time connectivity to external networks with a defined business requirement and using unidirectional networks with an air gap if possible.

- Physical security of medical devices is important – restricting physical access to controls is appropriate in some operating environments. This must be closely managed to ensure usability of systems is not adversely impacted.

- Expert cyber security services may be a helpful way in understanding how defendable the biomedical environment is – penetration testing can help to find vulnerabilities that could be exploited, and managed as part of an ongoing risk assessment.

The NIST framework outlined in Part 1, s.8 is readily applied to health and medical service situations. Good risk management can also be developed by applying relevant standards, shown in Table 4.

Table 4: Standards that may be applied by service providers

Standard	Scope
ISO 13485	Medical devices – Quality management systems
IEC/EN 62304	Medical devices – Software lifecycle requirements
IEC 80001	Application of risk management for IT-networks incorporating medical devices
ISO 15408	Evaluation criteria for IT security
IEC 82304	Health software - general requirements for product safety
ISO/IEC 30111	Resolve potential vulnerability information in a product
ISO/IEC 27000 series	Health informatics - Information security management in health using ISO/IEC 27002

Effective management of cyber security risks may assist to meet other regulatory compliance obligations in relation to information management, including under applicable privacy legislation.

Other factors for consideration

Cross functional collaboration

Collaboration is essential for effective cyber security control of medical devices in healthcare organisations.

Healthcare service providers should aim to facilitate an environment which drives cross functional collaboration between the biomedical, clinical support and IT teams, helping all areas to develop a better understanding of the work completed within each team.

The biomedical team should be incentivised to engage with medical professionals within the healthcare organisation to help broaden their understanding of the operating profile of their devices, the technology under their management, implementation of cyber security controls and the associated risk.

Collaborative procurement

Procurement is often a centralised task in healthcare providers. Asking the manufacturer and sponsor questions about cyber security and updating procurement practices to ensure the purchase of appropriately secure devices will create greater demand for improved cyber security within medical devices.

- Incentivise procurement teams to work with IT and biomedical teams on the procurement of new medical devices to provide informed advice on appropriate security measures for the specific healthcare service provider. This will help ensure that cyber security is a measurable factor in procurement.
- Questions to ask during the procurement process may include:
  - What security measures have been built into the device?
    - What measures are in place to protect patient safety?
    - What measures are in place to protect the confidentiality, availability and integrity of patient data?
    - How has security been addressed at the firmware level and at the user interface level?
  - What security protocols and frameworks have been used?
  - What are the known cyber security vulnerabilities for the device?
  - Has the manufacturer assessed the cyber security of key components within the device (i.e. the supply chain)?
  - Does the vendor provide an ongoing service to manage the security of the medical device(s)?
  - A medical device often has a long lifecycle – does the vendor have enough resources to support the security requirements throughout the lifecycle?
  - How is data from the device logged and stored? Are third party cloud services used and if so, what are their privacy and security policies? Is the data stored onshore?
  - How will the manufacturer respond in the future if a medical device cyber security incident occurs?

- – How has the company experienced any cyber security issues over the past 12 months and how were these managed?

Medical device inventory

To effectively manage cyber security risk, the organisation should consider developing an inventory and risk profile of the current state of connected medical devices, providing insight to vulnerabilities in the operating environment. The inventory should include:

- Medical device name, operation and purpose
- Any secondary uses beyond intended purpose
- Location of device and any restrictions on physical access
- Person responsible for device security
- Primary users of the device (and their cyber security training level)
- Level of device criticality
- Expected device life span
- Support agreements in place
- Refresh cycles
- Vendor and maintenance providers
- End-of-life procedure / support for critical components (e.g. OS, legacy protocols)

Cyber security training

Many professionals in the health and medical sector have received little training on cyber security.

- To ensure all staff are aware of the impacts that poor medical device cyber security practices could have, general training should be provided that raises baseline security awareness and skills of the whole staff cohort.
- Actively work to create a culture of cyber security awareness, vigilance and reporting, and regularly communicate potential cyber security issues within the biomedical team, and more broadly as appropriate. Encourage biomedical engineers to work with healthcare and medical professionals and other stakeholders as applicable, to understand cyber-safe practices for use of medical devices.
- Encourage senior biomedical engineers/technologists, to undertake professional development in cyber security, such as completion of industry standard cyber security training.

Segment the corporate network from the biomedical network

The corporate IT network should be segmented from the biomedical (medical devices) network. Ideally, this should be done with an internal firewall. This will significantly reduce the risk of malware spreading from one network to another. Medical devices should be segmented into logical groups (manufacturer or modality) to reduce the attack surface. When possible, medical devices should be isolated.

Regardless of the effort spent segmenting and isolating the biomedical network, compliance of the corporate network and broader health service IT system should be assessed against relevant cyber security standards on a regular basis.

Address legacy devices

Appropriately securing legacy medical devices is important, as in many cases, they were not manufactured with security as a priority, however, are increasingly becoming connected as the healthcare ecosystems take advantage of wireless technologies. If legacy devices do need to be connected to the network, if possible they should have their own dedicated and protected network, which is isolated from general IT assets and other medical devices.

Manage authentication

Access to the network is critical for most medical devices, especially with an Electronic Medical Record (EMR) system. Ensuring that only authenticated access is provided is key but when credentials are compromised, it can be challenging to define authenticated but unauthorised access.

- Consider implementing multi-factor authentication for staff access to networks, especially in areas of high traffic and reduce privileges to only those required.
- Ongoing remote access to devices post sale by medical device manufacturers and sponsors should be an exception, not the rule. Multi-factor authentication should be implemented with privileges reduced to only those required.
- Regular reviews of network access should be completed. These must be managed to ensure usability of systems is not adversely impacted.
- The use of hard-coded passwords and default accounts should be avoided.
- Sharing of credentials should be avoided. Ideally each user has their own account and credentials.

Secure remote access

- Only allowing remote access when required will limit the window of opportunity to adversaries.
- Restricted access when using applications remotely and time limited access should be considered.
- Multi-factor authentication is critical for remote access.

Restrict administrative privileges

- Adversaries primarily target user accounts with administrative privileges, as they have a high level of access to the organisation’s IT systems.
- Administrative privileges should be tightly controlled and only provided to those who need them. Consider making separate accounts with administrative privileges for these users which do not have access to the internet, as this reduces the likelihood of malware infection. Administrative accounts should not be used for regular use.
- Administrative account credentials should be changed following administrator staffing changes.

Monitor and respond

Monitoring the internal and external environment for medical device abnormalities and cyber security threats is important to building a stronger cyber security posture. One advantage of monitoring medical devices is that their range of normal operation is narrow. This means that anomalies can be easier to spot in medical devices than ICT equipment.

- Healthcare service providers should ensure they have visibility over their networks. Monitoring should occur in the following places:
  - Monitor IP traffic on biomedical network boundaries for abnormal or suspicious traffic
  - Monitor IP traffic within the biomedical network for malicious connections
  - Use host-based intrusion detection systems to detect malicious software and attack attempts
  - Use login analysis to detect stolen credentials usage or improper access, verifying all anomalies with quick phone calls
  - Watch account / user administration actions to detect access control manipulation such as elevating a user's privileges that would not normally require it
- Monitoring the broader environment for potential threats – this includes monitoring and responding to threat intelligence sources, such as CERT alerts and any alerts issued by the TGA, sponsor or manufacturer.
  - Service providers can apply threat information to manage risks according to standards and guidelines. The information can be applied to procurement process, hardening the security of the medical devices and their environment, or simple security audits in the form of regular penetration tests.

Cyber security and operational planning

Risk assessment and business continuity planning are key strategic operational activities undertaken by healthcare service providers and most small business operators.

- Ensure cyber security is proactively assessed as a key element in risk assessments and business continuity planning; proactively implementing appropriate cyber controls is essential to risk management.
- Develop a cyber security strategic plan, which includes a cyber specific risk assessment and response strategies. The plan should have clearly defined event response procedures that define the responsibilities of each department (in the hospital or other service provider) in the event of an incident, and emphasise the importance of each area being familiar with these procedures.

Reactive actions

Following a known or suspected cyber security breach via a medical device or on the biomedical network, service providers should be able to consult their cyber security strategic plan to understand the steps that need to be taken in the given situation. Some actions to consider include[28]:

- Work with clinicians to understand the implications of disabling network connectivity as a risk mitigation strategy on a case-by-case basis. If clinically acceptable, disconnect the medical device from the network.
- Work with clinicians to communicate any risks to patients, on a case-by-case basis. These risks may include the potential consequences of the breach, options to mitigate the risk, long term solutions to address cyber security breach and vulnerabilities, and discussion on the benefits of the device versus the cyber security risk.
- Work with cyber security team and the device manufacturer to contain the infection and to restore the system.
- If any unencrypted patient data was involved, inform risk management so that the potential breach can be handled in accordance with applicable obligations under the Privacy Act, including in accordance with the Notifiable Data Breach scheme and any related OAIC requirements.
- Avoid installing un-validated patches.
- Report the security breach to the device manufacturer or sponsor, and to the TGA as an adverse event if appropriate. The Australian Cyber Security Centre may also be a useful source of information to help overcome the breach.

Where appropriate, healthcare service providers might consider real time immersive scenario-based education and training to help prepare and build familiarity with the reactive actions required following a suspected breach. This will help build a security culture.

Measuring cyber security resilience

When considered collectively, the guidance provided for healthcare service providers can form the basis for assessing organisational maturity concerning medical device cyber security. This may be achieved by developing a matrix system, which can be used to understand areas of strength and areas where additional effort is required (e.g. Table 5). Healthcare service providers should develop low, medium and high criteria suitable to their organisation and assess maturity annually to ensure continued attention to providing a cyber security environment for the use of medical devices.

[28] ECRI Institute (2017). *Ransomware Attacks: How to Protect Your Medical Device Systems*, [Online] Available from: https://www.ecri.org/components/HDJournal/Pages/Ransomware-Attacks-How-to-Protect-Your-Systems.aspx. Accessed: 28/09/2018

Table 5: Example cyber security self-assessment matrix

Cyber security consideration	Low	Medium	High
Risk management strategy			
Cross functional collaboration			
Collaborative procurement			
Medical device inventory			
Cyber security training			
Network segmentation			
Address legacy devices			
Manage authentication			
Secure remote access			
Restrict administrative privileges			
Monitor and respond			
Cyber security and operational planning			
Reactive actions			

Note

An assessor should consider if there are established protocols and practices within the organisation, or how well they are established and implemented, across each of the cyber security considerations:

- **Low**: very little or emerging evidence of established policy and practice
- **Medium**: some policy and practices
- **High**: full implementation of cyber security policy and practice (e.g. alignment to international standards).

Appendix 1

Background

Cyber security in Australia

In 2016, the Australian Government released Australia's Cyber Security Strategy, detailing priority actions to improve Australia's general cyber security posture, alongside supporting the growth of the local cyber security industry[29]. Putting this into operation and providing a cyber secure environment that ensures stability for businesses and individuals to operate in is the responsibility of the Australian Government, specifically the Department of Defence and relevant agencies, including the Australian Signals Directorate (ASD) via the Australian Cyber Security Centre (ACSC). In line with this, the continued safety, quality and performance of medical devices impacted by cyber-related issues is the responsibility of the TGA.

Health technology and cyber security

The digitalisation of the health technology system (Appendix 1, Figure 3) is rapidly gathering traction, with increased application of wireless communication, cloud services, artificial intelligence (AI) and other technologies. Some of this technology meets the definition of a medical device, while some does not. Medical devices will increasingly be used in a wider variety of professional, personal and public environments, leading to new cyber security implications from an evolving cyber threat landscape.

Manufacturers and sponsors need to consider and plan for an evolving cyber security landscape to maintain patient safety. Table 6 highlights emerging social and technological trends that are affecting the cyber threat landscape and associated implications for the healthcare and medical device industry. The cyber-physical-human nature of many connected medical devices leads to cyber security vulnerabilities that cover traditional information security challenges, but also physical patient safety, though these are by nature difficult to predict. For example:

- Infusion pumps wirelessly connected to a number of systems and networks, introduce many cyber security vulnerabilities and threats, such as unauthorised access to health information and changes to the functionality of the device and prescription of drug doses[30].
- Digitalisation is blurring the distinction between medical devices and personal consumer devices, with smartphones able to act as the operational platform for some software based medical devices. Security of these devices relies on the user, often a patient, having up-to-date security software on their device and following cyber safe practices.

Beyond immediate patient harm, a single high profile adverse cyber event can disrupt professional and social trust in medical device advancement and the healthcare system more broadly, hindering innovation, development and deployment of digital health solutions for several years. Motivations for attacks on medical devices and associated networks may include:

- Financial and political gain through access to identity, financial and medical data stored in hospital IT systems or networks associated with medical devices, through selling of data, blackmail, etc.

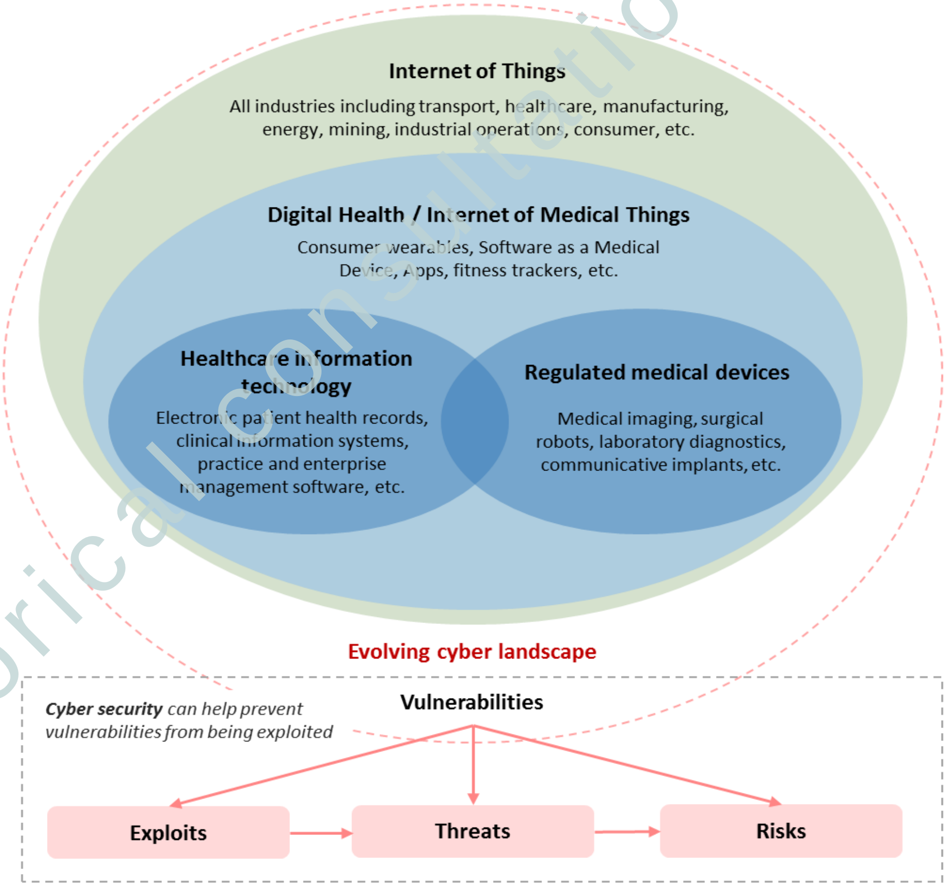
[29] Commonwealth of Australia (2016). *Australia's Cyber Security Strategy*, [Online] Available from: https://cybersecuritystrategy.homeaffairs.gov.au/. Accessed:28/09/2018

[30] NIST (2018). *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*, [Online] Available from: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf. Accessed: 28/09/2018

- Generating wide-scale disruption of services by gaining entry into hospital networks[31]
- Alteration or removal of a medical service or therapy to impact lives as a form of cyberwarfare, or targeting an individual
- Intellectual Property theft
- Impugning the reputation of a device manufacturer in order to alter market competition
- A motivation to harm other individuals
- Curiosity and prestige in demonstrating ability to debug complex systems to find and/or exploit vulnerabilities

Enabling medical devices to be cyber-secure is a requirement for regulatory compliance in Australia. Supporting greater cyber-maturity and resilience into Australia's medical device industry will improve the security culture of our healthcare industry and reduce the risk of devices causing patient harm through cyber vulnerabilities. To achieve this, medical device manufacturers and sponsors are also considering cyber security more broadly within their organisations, including workforce skills, strong leadership, and technology solutions.

Figure 3: The evolving digital health landscape


Internet of Things
All industries including transport, healthcare, manufacturing, energy, mining, industrial operations, consumer, etc.
Digital Health / Internet of Medical Things
Consumer wearables, Software as a Medical Device, Apps, fitness trackers, etc.
Healthcare information technology
Electronic patient health records, clinical information systems, practice and enterprise management software, etc.
Regulated medical devices
Medical imaging, surgical robots, laboratory diagnostics, communicative implants, etc.
Evolving cyber landscape
Cyber security can help prevent vulnerabilities from being exploited
Vulnerabilities
Exploits
Threats
Risks

- *Increased connectivity and digitisation of health technologies drives a changing cyber landscape, creating new vulnerabilities for medical devices.*
- *Likewise, vulnerabilities across the broader IT ecosystem can impact digital health technologies.*

[31] Frost & Sullivan (2016): Cyber security threats and medical device connectivity

Table 6: Healthcare and medical technology industry trends and cyber security implications

Trend	Cyber security considerations
Consumer control and experience • Patients are gaining more control over their healthcare and expecting quality experiences • Access to information is increasing consumer decision-making power and allowing proactive health management	• Devices providing better experiences for a patient are interacting with different environments (e.g. home or public Wi-Fi) and are exposed to a different threat landscape • Variable security literacy of patient / end-user
Integration of health service and supply chains • End-to-end integration of healthcare will improve efficiency and provide greater focus on the patient • Digital technologies are transforming supply chains, creating transparency and blurring traditional boundaries	• Interoperability of systems is needed for successful healthcare integration although this may introduce a new range of cyber security vulnerabilities • Security throughout the supply chain and other third parties is vital
Global Connectivity • Global connectivity is enabling trade; empowering people with access to information, products and services; and allowing seamless communication for improved social and professional connections • New entrants can scale-up quickly with access to global markets	• Cyber-attacks can come from anywhere in the world • Remote connection of physical devices introduces new cyber considerations – Internet of Things (IoT) vulnerabilities may include data but also extend to physical threats to health and safety
Precision and personal healthcare • Advances in science and technology, such as genome profiling and 3D printing are enabling technology solutions that are tuned to the specific needs of individuals • Bespoke technologies will provide improved outcomes for individual patients	• Precision healthcare can require the collection of lifestyle, personal health and medical information from a variety of sources, expanding the data that needs to be protected

Trend	Cyber security considerations
Increased data generation and exchange • Greater volumes of patient data are being generated and exchanged, enabling new insights and supporting new businesses and technologies • E.g. genome profiles will enable new diagnostic platforms	• Cyber security will need to ensure confidentially and integrity of this data is maintained Rapid data creation means that storage, and access controls are paramount
Healthcare: a targeted industry • Until recently, protective measures against cyber threats and investment into security within healthcare / medical technologies were limited[32] • Healthcare is vulnerable to cyber threats, with many poorly protected legacy systems in use • Cyber-attacks on healthcare organisations are increasing	• Adversaries have significant motivation to attack medical devices • Healthcare information is highly sought after on the dark web • Devices capturing, transmitting or storing health information should consider the risks created by poor cyber security

Legislative basis

The relevant Australian legislation and regulations for the regulation of medical devices includes:

- *Therapeutic Goods Act 1989* (the Act)
- *Therapeutic Goods Regulations 1990* (the TG Regulations)
- Therapeutic Goods (Medical Devices) Regulations 2002 (the MD Regulations)

Medical devices are classified according to the intended purpose of the device which generally correlates with the level of risk.

The classification of a medical device determines the options available to the manufacturer for demonstrating compliance with regulatory requirements prior to market authorisation, and to an extent the level of review by the TGA and/or certification bodies (e.g. European Notified Bodies) in the conformity assessment process.

Regardless of the classification of the device, the manufacturer is required to generate and maintain evidence regarding the quality management systems and risk management frameworks used to manage medical device cyber security to demonstrate compliance of the device(s) with the Essential Principles.

[32] Lynne Coventry, Dawn Branley (2018). *Cybersecurity in healthcare: A narrative review of trends, threats and ways forward* - https://t.co/3PC9WDObfg

Note

A medical device must comply with the Essential Principles which set out the requirements relating to safety and performance. The Act and MD Regulations also require that the sponsor must have available sufficient information to substantiate compliance with the Essential Principles or have procedures in place with the manufacturer that will allow them to obtain such information and provide this information to the TGA if required.

The obligation to have information that demonstrates compliance with the Essential Principles lies with the manufacturer of the device. However the sponsor must be able to provide information to TGA to demonstrate such compliance. This applies to all medical devices regardless of risk class.

Appendix 2

Definitions

Adversary – an entity, individual or group that seeks to target a digital system to find vulnerabilities. There are two classes of adversarial capabilities:

- **White hat hackers**, who assess a target system to find its vulnerabilities (known or new), may implement "exploits" to test these vulnerabilities and follow ethical rules to report their findings.
- **Black hat adversaries**, who assess a target system to find its vulnerabilities (known or new), implement "exploits" for these vulnerabilities and use exploits to attack the system with malicious motivation.

Attack surface – the different points (code, components, user functions, etc.) where a medical device is exposed to adversaries or other unauthorised modifications.

Australian Register of Therapeutic Goods (ARTG) – a register for the purpose of compiling information in relation to, and providing for evaluation of, therapeutic goods for use in humans.

Computer Emergency Response Team (CERT) – expert groups that provide assistance in handling security incidents.

Cyber security – the processes, techniques and technologies employed to defend medical devices and their associated systems from digital attacks or inadvertent misuse. This includes preventing unauthorised access, modification, misuse or denial of use of digital medical devices, and preventing the unauthorised use of information that is stored, accessed, or transferred to or from the medical device.

Digital health – electronic technologies, including medical devices, which can be used by clinicians to improve workflow and enhance service delivery. The technologies can also be used by individuals to support them in playing a proactive role in their health and wellbeing to meet short- or long-term lifestyle goals.

Essential Principles – set out the requirements relating to the safety and performance characteristics of medical devices. Compliance with applicable medical device standards is not required by the legislation, but it is one way to demonstrate compliance with Essential Principles[33]. The Essential Principles are defined in Schedule 1 of the *Therapeutic Goods (Medical Devices) Regulations 2002*.

Exploit – an instance where a vulnerability or vulnerabilities have been exercised (accidently or intentionally) by a threat and could impact the safety or essential performance of a medical device or use a medical device as a vector to compromise a connected device or system[34].

Internet of Things (IoT) – a term that describes the physical devices that connect to the internet, and to each other. The IoT includes medical devices that may be connected to other medical devices or to other internal (to an organisation) or external networks.

Malware – software designed with malicious intent to disrupt normal function of a system or device, gather sensitive information, and/or access other connected systems[35].

[33] Section 41C, Therapeutic Goods Act 1989

[34] US Food and Drug Administration (2016): *Postmarket Management of Cybersecurity in Medical Devices* https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

Manufacturer of a medical device – According to the *Therapeutic Goods Act 1989*[36]:

1. The ***manufacturer*** of a medical device is the person who is responsible for the design, production, packaging and labelling of the device before it is supplied under the person's name, whether or not it is the person, or another person acting on the person's behalf, who carries out those operations.

2. If subsection (1) does not apply to a medical device, the ***manufacturer*** of the device is the person who, with a view to supplying the device under the person's name, does one or more of the following using ready-made products:

   a. assembles the device;

   b. packages the device;

   c. processes the device;

   d. fully refurbishes the device;

   e. labels the device;

   f. assigns to the device its purpose by means of information supplied, by the person, on or in any one or more of the following:

      i. the labelling on the device;

      ii. the instructions for using the device;

      iii. any advertising material relating to the device;

      iv. technical documentation describing the mechanism of action of the device.

3. However, a person is not the manufacturer of a medical device if:

   a. the person assembles or adapts the device for an individual patient; and

   b. the device has already been supplied by another person; and

   c. the assembly or adaptation does not change the purpose intended for the device by means of information supplied by that other person, on or in any one or more of the following:

      i. the labelling on the device;

      ii. the instructions for using the device;

      iii. any advertising material relating to the device;

      iv. technical documentation describing the mechanism of action of the device.

[35] US Food and Drug Administration (2018): *Content for Premarket Submissions for Management of Cybersecurity in Medical Devices* – *https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf*

[36] Section 41BG, Therapeutic Goods Act 1989

Medical device

1. A ***medical device*** is:

   a. any instrument, apparatus, appliance, material or other article (whether used alone or in combination, and including the software necessary for its proper application) intended, by the person under whose name it is or is to be supplied, to be used for human beings for the purpose of one or more of the following:

      i. diagnosis, prevention, monitoring, treatment or alleviation of disease;

      ii. diagnosis, monitoring, treatment, alleviation of or compensation for an injury or disability;

      iii. investigation, replacement or modification of the anatomy or of a physiological process;

      iv. control of conception;

      and that does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but that may be assisted in its function by such means; or

   aa. any instrument, apparatus, appliance, material or other article specified under subsection 41BD(2A) of the Act; or

   ab. any instrument, apparatus, appliance, material or other article that is included in a class of instruments, apparatus, appliances, materials or other articles specified under subsection 41BD(2B) of the Act; or

   b. an accessory to an instrument, apparatus, appliance, material or other article covered by paragraph (a), (aa) or (ab).

Non-recall actions – a type of action taken if therapeutic goods meet all specifications and standards and there are no deficiencies in safety, quality, efficacy, performance or presentation[37].

Patient harm – physical injury or damage to the health of patients, including death. Cyber security exploits (e.g. loss of authenticity, availability, integrity, or confidentiality) of a device may pose a risk to health and may result in patient harm[38].

Recall – a type of regulatory action that is taken to protect the health and safety of consumers from therapeutic goods that are, or may be, affected by an issue with a therapeutic good in relation to its quality, safety, efficacy (medicines and biologicals), performance (medical devices) or presentation[39].

[37] Uniform Recall Procedure for Therapeutic Goods, V2.0, October 2017 - https://www.tga.gov.au/publication/uniform-recall-procedure-therapeutic-goods-urptg-v20

[38] US Food and Drug Administration (2018): *Content for Premarket Submissions for Management of Cybersecurity in Medical Devices* - *https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf*

[39] Uniform Recall Procedure for Therapeutic Goods, V2.0, October 2017 - https://www.tga.gov.au/publication/uniform-recall-procedure-therapeutic-goods-urptg-v20

Risk – Risk is defined as the combination of the probability of occurrence of harm and the severity of that harm. In terms of cyber security, the existence of a threat and the likelihood of it being exploited towards a medical device that would result in the device losing its value to its owner is a risk. This value may change from owner to owner: e.g. for consumers, values include wellbeing, safety, privacy or cost; for health services, values include liability, prestige and profit; for industry, values include profit, prestige, and market share and business continuity; and for governments, values include the safety of citizens and cost.

Software as a Medical Device (SaMD) – software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device[40].

- SaMD is a medical device itself and includes in-vitro diagnostic (IVD) medical device. It is capable of running on general purpose (non-medical purpose) computing platforms. The term 'without being part of' means software not necessary for a hardware medical device to achieve its intended medical purpose.
- Software does not meet the definition of SaMD if its intended purpose is to drive a hardware medical device.
- SaMD may be used in combination (e.g., as a module) with other products including medical devices. SaMD may be interfaced with other medical devices, including hardware medical devices and other SaMD software, as well as general purpose software.
- Mobile apps that meet the definition above are considered SaMD.

Sponsor[41]

> ***sponsor***, in relation to therapeutic goods, means:
>
> a. a person who exports, or arranges the exportation of, the goods from Australia; or
>
> b. a person who imports, or arranges the importation of, the goods into Australia; or
>
> c. a person who, in Australia, manufactures the goods, or arranges for another person to manufacture the goods, for supply (whether in Australia or elsewhere);
>
> but does not include a person who:
>
> d. exports, imports or manufactures the goods; or
>
> e. arranges the exportation, importation or manufacture of the goods;
>
> on behalf of another person who, at the time of the exportation, importation, manufacture or arrangements, is a resident of, or is carrying on business in, Australia.

System kernel – this is the central code of an operating system, managing the core operation of the computer and hardware, most critically computer memory and the central processing unit (CPU).

[40] International Medical Device Regulators Forum (2013): *Software as a Medical Devices (SaMD): Key Definitions* - http://www.imdrf.org/documents/documents.asp

[41] Section 3, Therapeutic Goods Act 1989

Threat – any circumstance or event with the potential to adversely impact the device, organisational operations (including mission, functions, or reputation), organisational assets, individuals, or other organisations through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service. Threats exercise vulnerabilities, which may impact the safety or essential performance of the device[42].

Vulnerability – a weakness in an information system, system security procedures, internal controls, human behaviour, or implementation that could be exploited by a threat[43].

[42] US Food and Drug Administration (2016): *Postmarket Management of Cybersecurity in Medical Devices*. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[43] Food and Drug Administration (2016): Postmarket Management of Cybersecurity in Medical Devices.

Appendix 3

Other guidance materials

This draft Australian regulatory guidance for medical device cyber security aims to harmonise with relevant international guidance. This should facilitate the import and export of medical devices to and from Australia. There are also a number of guidance documents on the cyber security of medical devices that have been published or under development by international medical device regulators.

In the USA, the FDA's Centre for Devices and Radiological Health (CDRH) has published several guidance documents that are relevant for cyber security. These are available on the FDA website:

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (pdf,324kb)
- Post market Management of Cybersecurity in Medical Devices (pdf,1.23Mb)
- Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices (pdf,165kb)
- Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software (pdf,165kb)
- Deciding When to Submit a 510(k) for a Software Change to an Existing Device (585kb)
- Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices, (pdf,650kb)
- Mobile Medical Applications (pdf,1.28Mb)

Also in the USA, the National Institute of Standards and Technology (NIST), through its National Cybersecurity Centre of Excellence (NCCoE) has produced Cyber Security Practice Guides for various industries, including healthcare:

- Securing Electronic Health Records on Mobile Devices
- Securing Wireless Infusion Pumps

The International Medical Device Regulators Forum (IMDRF) has worked to further a unanimous understanding of challenging topic areas, such as SaMD[44], which have a high risk of being exposed to malicious cyber activity. In addition, IMDRF has recently formed a working group to directly address cyber security. Relevant documents are available on the IMDRF website (in both PDF and DOCX formats), and include:

- Software as a Medical Device (SaMD): Key Definitions (docx,68kb)
- Software as a Medical Device (SaMD): Possible Framework for Risk Categorization and Corresponding Considerations (docx,176kb)
- Software as a Medical Device (SaMD): Application of Quality Management System (docx,749kb)

[44] IMDRF (n.d.): *Software as a Medical Device (SaMD)*, [Online] Available from: http://www.imdrf.org/workitems/wi-samd.asp. Accessed: 28/09/2018

- Software as a Medical Device (SaMD): Clinical Evaluation (docx,1.13Mb)

In Europe, the new Medical Device Regulation has introduced a specific requirement for cyber security for medical devices. This Regulation, (EU) 2017/745, will be fully implemented by 2020. More broadly, the European Union Agency for Network and Information Security (ENISA) has published guidance on baseline security for IoT:

- Baseline security recommendations for IoT in the context of critical information infrastructures

In other jurisdictions, authorities external to health departments are investigating cyber security approaches for a range of IoT devices, including connected medical devices, e.g. South Korea's Ministry of Science and ICT together with the Korea Internet and Security Agency (KISA) released a 'Cyber Security Guide for Smart Medical Service' which aims to address security threats that may arise in smart medical services and how to respond to them[45].

The ECRI Institute, an independent non-profit organisation that researches approaches to improving patient care, has significant global activity in medical device cyber security and has published a series of relevant subscription based guidance documents (log in required):

- Cybersecurity Risk Assessment For Medical Devices
- Cyber Threats Top ECRI Institute's 2019 Health Technology Hazards
- Cybersecurity: The Essentials
- Anti-Malware Software And Medical Devices: A Crash Course In Protecting Your Devices From Cyber Attacks
- Ransomware Attacks: How To Protect Your Medical Device Systems

[45] KISA (2018): *Cyber Security Guide for Smart Medical Service*, [Online] Available from: http://www.kisa.or.kr/uploadfile/201805/201805290956314977.pdf. Accessed: 23/07/2018

Appendix 4

Cyber security intelligence and threat sharing

To ensure that a medical device included in the ARTG continues to meet the requirements of the Essential Principles, a manufacturer or sponsor must demonstrate how they will gather information regarding emerging cyber security vulnerabilities that may impact the safe operation of their medical device and how these will be addressed. Manufacturers should also share information with the TGA, see section on post market, and the wider industry regarding cyber security vulnerabilities and threats that they discover.

This can be achieved by ensuring that complaint monitoring processes for sponsor and manufacturers include cyber security issues. In addition, manufacturers should aim to monitor threat-sharing websites or join informal intelligence sharing groups.

In Australia, cyber security threat information sharing and monitoring can be facilitated through CERT Australia (operated under the Joint Cyber Security Centres as part of the ACSC) and AusCERT (not-for-profit organisation under the University of Queensland). Internationally, the US based ICS-CERT provides regular updates concerning known medical device threats.

Additional entities that focus on cyber security intelligence and threat sharing include:

- The Trusted Information Sharing Network (TISN), which includes a Health Group for sharing cyber security threat information relevant to the health and medical sector. TISN have published a number of documents that are relevant to cyber security threat sharing.
- The IoT Alliance Australia includes a specific work stream dedicated to cyber security and network resilience, and is in the process of developing a health focused work stream.

Effective threat intelligence sharing within medical device developers, manufacturers, sponsors and users should consider the following:

- Software, hardware and protocol vulnerabilities
- Exploits, methods or tools which are developed to take advantage of one or more vulnerabilities
- Risk associated with the existing vulnerabilities, exploits and threats
- Incidents where known or unknown exploits are used to realise the threat
- Recovery or mitigation strategies

Appendix 5

Frameworks and standards from other sectors

Changes in the cyber security risk landscape will continue to change approach to managing cyber security for medical devices. Manufacturers and sponsors are encouraged to assess and understand emerging cyber security standards and frameworks from industries that share similarities with the medical devices ecosystem. This might include defence and financial services where operational security and privacy are primary drivers, or the broad Internet of Things community within which connected medical devices are implicitly included (Appendix 1, Figure 3). Table 7 provides a selection of frameworks and standards that may be of interest to medical device manufacturers and sponsors seeking to include a device on the ARTG in Australia.

Table 7: Emerging cyber security frameworks from adjacent industries

Organisation, year	Name of Document	Summary
Internet of Things (IoT)		
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT, in the context of critical information infrastructures	This focuses on security considerations rather than standards.
IEEE Standards Association	Internet of Things Related Standards Medical device communications	A comprehensive list of IoT standards Protocols for information exchange
National Institute of Standards and Technology (NIST), U.S. Department of Commerce, 2018	Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)	Covers connected vehicles, consumer IoT, Health IoT, smart buildings, smart manufacturing Looks at cybersecurity risks as well as standards
Industrial Control Systems (ICS)		
ISA/IEC-62443 series of standards	Industrial Automation and Control Systems Security	Define procedures for implementing electronically secure manufacturing and control systems and security practices and assessing electronic security performance

NIST, 2015	NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security	Guidance on how to secure ICS, including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements.
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 2016	Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies	Strategies for defence and recommendations for securing ICS
Financial services		
World Bank Group, 2017	Financial Sector's Cybersecurity: A regulatory Digest	A compilation of recent cybersecurity laws, regulations, guidelines and other significant documents on cybersecurity for the financial sector.
Defence		
Defence Federal Acquisition Regulation Supplement (DFARS)	Defence Federal Acquisition Regulation Supplements (DFARDS) and Procedures, Guidance and Information (PGI)	DFARS outlines cybersecurity standards a third party must meet and comply with prior to doing business with the Department of Defence in order to protect sensitive defence information.

Appendix 6

Examples of known medical device cyber security vulnerabilities

Medical device cyber security vulnerabilities

- Accepts untrusted input
- Authentication bypass
- Buffer overflow
- Code injection
- Communication protocol vulnerability
- Cross-site scripting
- Cryptographic issues
- Debug service enabled by default
- Default password
- Exposed dangerous method or function
- Hard-coded credentials
- Improper access control
- Improper authentication
- Improper authorisation
- Improper certificate validation
- Improper control of generation code
- Improper exception handling
- Improper input validation
- Improper restriction of communication channel to intended endpoints
- Improper restriction of operations within the bounds of a memory buffer
- Improper restriction of power consumption
- Improper restriction of XML external entity
- Reference information exposure
- Insufficient session expiration
- Insufficient verification of data authenticity
- Insufficiently protected credentials
- Insufficiently protected flash memory content
- Leftover debug code
- Man-in-the-middle
- Meltdown and Spectre
- Missing confidentiality
- Numeric errors
- Out-of-bounds read
- Path traversal
- PC operating system vulnerabilities
- Protection mechanism failure
- Relative path traversal
- Resource management errors
- Uncontrolled resource consumption
- Uncontrolled search path element
- Unquoted search path or element
- Vulnerable third-party software
- Weak password hashing algorithm

Sources: ICS-CERT, AusCERT, CERT Australia

Appendix 7

Consumer Factsheet - Medical Device Cyber Security

Safely using connected and digital medical devices

Digital technology in your medical devices

You may have noticed that some of your medical devices can connect to the internet, communicate with your mobile phone, or send data to a third party such as the device manufacturer or your doctor.

These features, enabled by digital technology, aim to make these devices more useful. They can help you control the device, monitor your health at home, or share data that your doctor might use to treat you.

Some examples of medical devices with digital technology include:

- apps on your smartphone that allow you to monitor a condition, such as monitoring headache frequency and severity
- implanted devices that can be remotely controlled, such as cardiac pacemakers
- hearing aids that may be controlled by your smartphone
- and continuous positive airway pressure (CPAP) machines that provide you with therapy and communicate therapy data to your doctor.

What can you do to ensure cyber security of your medical devices?

The digital features of these medical devices can affect the safety of the device if the right precautions aren't taken. So it's important to protect your medical device and the data it generates.

To maintain safety for these devices, cyber security is an important consideration. Cyber security includes the protections you put in place to secure your device and your home's digital environment, as well as your online conduct such as the websites you visit, the surveys you take, and the passwords you use.

How can I secure my medical device?

- ***Follow instructions when using your device*** – You should always read the information provided with your medical device, including its instructions for safe use and maintenance, its intended purpose and any limitations associated with its use. If you have misplaced or do not understand the information provided with the medical device and are concerned that this may affect your cyber safety, talk with your doctor.
- ***Protect your device throughout its lifespan*** – It is important that you continue to keep your medical devices up-to-date with the latest version of software. This is to ensure that the device remains as cyber secure as possible in the event of new cyber security issues. You doctor or the device manufacturer will have information on the latest updates available for your device. Always be careful when using your medical device outside a home environment. If possible avoid connecting to public networks that can be accessed by many people. If you cannot avoid connecting to a public network, try to minimise sending or receiving sensitive information during this period.

- ***Use passphrases*** – The password that comes with your medical device may not be strong enough. To improve your protection, change from a password to a hard-to-guess passphrase. A passphrase is a phrase that only you are likely to know and that is easy for you to remember, but hard for someone else to guess (e.g. YellowSubmarine527).

- ***Turn off features that you do not use*** – Your device might have some communicating capabilities that you don't always use or need. One example is a Bluetooth capability that automatically allows your device to connect to your computer or a nearby WIFI network. If you do not use this feature or only use it sometimes, you should turn the feature off when not needed. You should speak to your doctor before turning off any features.

How can I secure my digital environment?

- ***Secure your computing devices*** – Using the internet on your personal computer, laptop, tablet or smartphone can affect the security of your network, which in turn can affect your medical device if it is connected to this same network. Using security features on your computing device is important. These security features include the use of a passphrase or pin to unlock the device, making sure that your devices have current security software and keeping your software updated when prompted by your device.

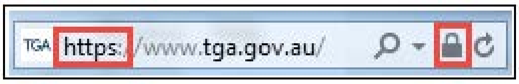
- ***Use backups and protection*** – We all store a lot of precious data on our computers, such as photos and important documents. Your medical device might also be storing valuable data for your healthcare. Creating backups of your data can help you recover if something does go wrong. This involves creating an extra copy of your data on a storage device, such as a USB or external hard drive, or to a reputable online cloud service. For further information see www. staysmartonline.gov.au

What behaviours are cyber smart?

- ***Pay attention to privacy*** – Sometimes you might share information when you use your medical device, with either a health professional or the company that makes the device. If medical devices do this automatically, it should be disclosed in the user manual or information, if not ask your doctor or the manufacturer of your device. You may also be sharing information about your health management in online forums with people who have similar health conditions. Always think about the type of information you are sharing with people, and ask yourself why someone needs that information. Consider if the people you are giving your data to are secure. How will sharing your data affect your security and what benefit will you receive by sharing. For further information see www.staysmartonline.gov.au

- ***Be aware of suspicious messaging*** – Sometimes your doctor or your medical device will communicate to you via an electronic message, such as a text message, email, chat function or web portal. Hackers might try to replicate this messaging to obtain your information, or get you to click on a link that could break the integrity of your device. You should exercise caution and ensure that the message is from a trusted person before acting on any information contained within it. If in doubt, do not respond and contact you doctor or the medical device manufacturer using contact details listed in a place other than within the suspicious message.

- ***Browse responsibly*** – Some webpages can be unsafe and can affect your computer just by visiting them. You should minimise visits to unknown websites and look for the padlock symbol and 'https' in the browser address when visiting websites. For further information see www. staysmartonline.gov.au



How you can report

ℹ If a medical device appears to have been impacted by a cyber security issue and could directly impact your health or safety, you should **report this as soon as possible** to your general practitioner, and also directly to the TGA.

Not every report made to the TGA requires action. However, reports are one important source of information for the TGA to assess the safety, quality and performance of medical devices. Therefore, when you submit a report to the TGA, even if there is no direct outcome for you, you are contributing to the ongoing collection of information that helps ensure the safety, quality and performance of medical devices in Australia.

You can report online; or by phone, email or post. Visit www.tga.gov.au and follow the link to Report a problem.

Version history

Version	Description of change	Author	Effective date
V1.0	Original publication – for consultation	Therapeutic Goods Administration, Medical Devices Branch	19/12/2018

Therapeutic Goods Administration

PO Box 100 Woden ACT 2606 Australia
Email: info@tga.gov.au Phone: 1800 020 653 Fax: 02 6203 1605
https://www.tga.gov.au

Reference/Publication #