Australian Government

Department of Health and Aged Care

Therapeutic Goods Administration

Medical device cyber security guidance for industry

Version 1.2, November 2022

Copyright
© Commonwealth of Australia 2022
This work is copyright. You may reproduce the whole or part of this work in unaltered form for your own personal use or, if you are part of an organisation, for internal use within your organisation, but only if you or your organisation do not use the reproduction for any commercial purpose and retain this copyright notice and all disclaimer notices as part of that reproduction. Apart from rights to use as permitted by the *Copyright Act 1968* or allowed by this copyright notice, all other rights are reserved and you are not allowed to reproduce the whole or any part of this work in any way (electronic or otherwise) without first being given specific written permission from the Commonwealth to do so. Requests and inquiries concerning reproduction and rights are to be sent to the TGA Copyright Officer, Therapeutic Goods Administration, PO Box 100, Woden ACT 2606 or emailed to <tga.copyright@tga.gov.au>.

Contents

Introduction 5

Connectivity and digitisation increase benefits and risks 5

Purpose and scope of this guidance 6

Lifespan of a medical device 6

Risk assessment and management 6

Total product lifecycle guidance 7

Total product life cycle (TPLC) 7

Essential Principles 8

About the Essential Principles 8

Compliance with the Essential Principles 8

Compliance throughout lifecycle 9

Cyber security risks and the Essential Principles 10

Relevant standards 15

Cyber Security Key Terms 23

Vulnerabilities 23

Exploits 23

Threats 23

Cyber security risk monitoring 24

Pre-market guidance 25

Pre-market regulatory requirements 25

Development approach 25

Application of standards 26

Risk management strategies 27

Management of manufacturing and supply chain 29

Provision of information for users 30

Technical cyber security considerations 31

Modularised design architecture 31

Cyber security assessment and penetration testing 31

Operating platform security 33

Update pathways 33

Trusted access and content provision 33

Post-market guidance 34
Regulatory requirements 34
Cyber security risk 36
Cyber security threat and risk response 36
Monitoring issues 36
Risk assessment 37
Updates and change control 38
Uniform recall procedure for therapeutic goods (URPTG) 39
Cyber security intelligence and threat sharing 41
Manufacturers and sponsors 41
Appendix 1: Known vulnerabilities 43
Appendix 2: The evolving cyber security landscape 45
Cyber security in Australia 45
Health technology and cyber security 45
The role of the TGA 46
Manufacturer and sponsor responsibilities 47
Motivations for malicious activity 47
Industry trends and cyber security considerations 48
Appendix 3: Frameworks and standards related to cyber security from other sectors 51
Internet of things (IoT) 51
Industrial control systems (ICS) 51
Financial services 52
Defence 52
Appendix 4: International guidance on medical device cyber security 53
USA guidance 53
IMDRF guidance 54
European guidance 54
Other jurisdictions 54
Glossary 55

Introduction

This guidance is for manufacturers and sponsors of medical devices that include software or electronic components.

The guidance is intended for:

manufacturers that develop software for use in or as standalone medical devices, such as in Software as a Medical Device (SaMD); this includes devices that incorporate artificial intelligence in their design

- manufacturers of medical devices (including in-vitro diagnostic medical devices) where devices include components that may be vulnerable to cyber-based threats
- medical device 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

Alongside this guidance, the TGA has also produced medical device cyber security guidance for users.

The Australian government regularly provides updates and advisories on cybersecurity for Australian organisations at cyber,gov,au. The TGA recommends that medical device sponsors and manufacturers consult cyber.gov.au for the latest advice on various cybersecurity issues and education from Australian government.

It is noted that an advisory was issued in April 2022 for Australian organisations to urgently update their cybersecurity posture.

Connectivity and digitisation increase benefits and risks

Connectivity and digitisation of medical device technologies may help improve device functionality and benefit. However, the connection of medical devices to networks or the internet exposes them to increased cyber threats that can potentially lead to increased risk of harm to patients. These might include:

- denial of intended service or therapy
- alteration of device function to directly cause patient harm
- loss of privacy or alteration of personal health data

Additionally, there are fundamental security interdependencies between medical devices and the networks they connect to. Cyber security for medical devices must be considered as part of a layered, holistic security ecosystem. The cyber security landscape is constantly evolving.

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 of this guidance

This guidance has been produced in order to support Australia's medical device cyber security capability, embedding improved cyber security practices across the medical device sector. This guidance on cyber security for medical devices is in line with existing regulatory requirements and 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.

The purpose of this guidance is to help manufacturers and sponsors understand how the TGA interprets regulations, and thus indicate how to comply. This is a guide only, and manufacturers and sponsors are encouraged to familiarise themselves with the legislative and regulatory requirements in Australia. If necessary, seek professional advice as it is the responsibility of each manufacturer or sponsor to understand and comply with these requirements.

This document will evolve over time and updates and clarifications will be included as required. Feedback on the guidance is always welcome.

Lifespan of a medical device

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
- end-of-life / withdrawal of support

Adopting a total product life cycle (TPLC) approach to risk and quality management is required.

Risk assessment and management

Assessment and management of cyber security risks that could compromise the health and safety of a patient, user or any other person, as with other risks for medical devices, is the responsibility of the manufacturer. At a minimum, it is expected that manufacturers have consulted cyber.gov.au and ensured that the most up to date advice from Australian government has been incorporated into their risk assessment and management strategy.

- **Pre-market:** Manufacturers are required to address cyber security risks during the design and development process. This includes:

  - general considerations, such as the development approach; administration protocols; application of standards; risk management strategies; infrastructure, manufacturing and supply chain management; and provision of information for users
  - technical considerations, such as cyber security penetration testing; modularised design architecture; operating platform security; emerging software; and Trusted access and content provision
  - environmental considerations for the device's intended use, such as connecting to networks, and uploading or downloading data
  - physical considerations, such as mechanical locks on devices and interfaces, physically securing networks, waste management (preventing capture of sensitive paper-based information)
  - social considerations, such as designing out or minimising social-engineering threats (e.g., phishing, impersonation, baiting, tailgating)
- **Post-market:** Manufacturers and sponsors are required to continually assess and take action on medical device cyber security risk
  - The cyber security threat landscape changes in short periods of time, therefore a compliant risk management strategy will demonstrate how medical device cybersecurity risk is reviewed and updated.
  - Cyber security events that do not appear to immediately impact a medical device are still part of the cyber security threat landscape, and will need to be considered as part of a compliant medical device cyber security risk management strategy.

Total product lifecycle guidance

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 may 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, controlled and documented across all phases in the life of a medical device, from the initial conception to development and testing, market authorisation, post-market use, and through to end-of-life and obsolescence. Meeting these expectations is most readily achieved by adopting a total product life cycle (TPLC) approach to risk and quality management. One standard that may be consulted to help with this is IEC 62304 (detailed in Relevant Standards).

As with other risks, if cyber security risk is not effectively minimised or managed 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 including:

- risk management procedures
- change management procedures
- design procedures
- complaint management procedures

As clinical use of a medical device is sometimes considerably longer than the expected lifespan of the technology that allows its operation (e.g. software and connectivity hardware), manufacturers and sponsors need to be aware of this challenge and work with users to effectively minimise risk.

Essential Principles

About the Essential Principles

For a medical device to be included on the ARTG, the manufacturer must demonstrate compliance with the Essential Principles. **The Essential Principles require that a manufacturer minimise the risks associated with the design, long-term safety and use of the device; this implicitly includes minimisation of cyber security risk.**

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 *Therapeutic Goods (Medical Devices) Regulations 2002* – Schedule 1 for more information).

The Essential Principles are not a prescriptive list of requirements for manufacturers to comply with and instead provide high level principles for flexibility according to the characteristics of the device. The legislation does not mandate the means by which a manufacturer must prove that they have met the Essential Principles. It is a manufacturer's responsibility to determine which essential principles are relevant and to demonstrate compliance with these.

Compliance with the Essential Principles

A medical device must comply with the Essential Principles which set out the requirements relating to safety and performance. 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 Relevant Standards). Supplying 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[1].

- 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, regardless of the classification of the device
- 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 requested.

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 the TGA to demonstrate such compliance. This applies to all medical devices regardless of risk class.

Compliance throughout lifecycle

Throughout the medical device life cycle, manufacturers need to ensure continuing compliance with the Essential Principles. Risk management for medical device cyber security requires assessment and corresponding 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 because of the share responsibility of cybersecurity, medical device users may represent a potential threat.
- Medical devices can be used by an attacker as a threat vector into their associated networks.
- The cyber security threat landscape is rapidly evolving and requires constant monitoring and appropriate corrective and preventative action from medical device manufacturers and sponsors, alongside cooperation or coordination with medical device users.
- Potential harm to patients and users from an adverse medical device cyber security event could clearly include physical harm (e.g. a device no longer operating as intended). There may also be other consequences for patients, users and the general community arising from a cyber security event related to a medical device, including for example, psychological harm, incorrect diagnosis, breaches of privacy through the disclosure of personal information, or financial consequences.
- Personal health data, including data collected from medical devices, presents a lucrative target for malicious activity, requiring secure storage and transmission solutions.
- 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 often receives less frequent patches over time, or becomes officially unsupported.

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

Cyber security risks and the Essential Principles

As a cyber security risk can be a safety concern, consideration and minimisation of such risks are imperative to compliance with many of the Essential Principles.

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:

- identify hazards and associated risks associated both its intended purpose and foreseeable misuse of the device
- eliminate or reduce the identified risks as far as possible by adopting a policy of inherently safe design and construction
- ensure adequate protection measures are taken, including alarms if necessary, in relation to any risks that cannot be eliminated
- inform users of any residual risks that may arise due to any shortcomings of the protection measures adopted

Essential Principle 12.1 (5)[2] requires that manufacturers of programmed or programmable medical devices, or software that is a medical device, design, produce and maintain with regard to best practice in relation to software, security and engineering to provide cybersecurity of the device, including to:

- provide protection against unauthorised access, unauthorised influence or unauthorised manipulation
- minimise risks associated with known cybersecurity vulnerabilities
- facilitate the application of updates, patches, compensating controls and other improvements, including making available sufficient information for a user to make decision with respect to the safety of applying or not applying these
  - disclose known vulnerabilities in the device or its components and associated mitigations

Cyber security considerations that a manufacturer may need to address to comply with these Essential Principles will depend on the type of device, but may include:

- off-label use of devices by clinicians in certain situations
- malicious and unauthorised access to or modification of a device
- exploitation of known vulnerabilities in the device software or hardware

[2] The revised Essential Principle 12.1 came into effect on 25 February 2021. Its represents the TGA's current expectations regarding cyber security for devices of this type.

- 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

Additional examples of cyber security considerations for manufacturers and sponsors as they relate to a number of the Essential Principles are highlighted in Table 1. Where appropriate, these considerations require the manufacturer to act to reduce or manage associated risk and these actions should be documented in the manufacturer's quality management system and/or risk management system.

Table 1: Relevant Essential Principles and their cyber security considerations

Essential Principle	Cyber security considerations
1. Use of medical devices not to compromise health and safety	• Does the intended use of the device expose it to risks associated with cyber security (e.g. will the device connect to networks, will it transmit data)? How will any cyber risks be managed? • Is there risk that a cyber security vulnerability may lead to the medical device compromising the health and safety of the user (patient or operator)? Is that risk acceptable? • Is there risk that the device could compromise the safety and health of other people (e.g. could the device compromise a biomedical network with other connected medical devices?) • Is it reasonable to expect the intended users would have appropriate technical knowledge, experience, education or training to use the device in a way that manages cyber security risk? Is the device adequately secured to limit risk of falsification, impersonation or suppression of data generated?
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, or the products it connects to, and does product development meet this? • Has cyber security been considered across the total product lifecycle of the device, and in consideration of the different expected user environments? • 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?

Essential Principle	Cyber security considerations
	Does this risk assessment consider risks associated with the implementation of selected security controls (e.g. application of security patches to devices post-market)? • If appropriate, does the device have the capability to detect, notify and log cyber security issues and raise an alarm if at risk? • What is the usability of the cyber security functionality within the device? Is there risk associated with applying security updates? To ensure continual compliance with Essential Principle 2, is there a plan in place to ensure timely responses to industry known vulnerabilities?
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? • Does the device's intended purpose stay validated when the network/network components are updated?
4. Long-term safety	• Is the cyber security of the device able to be regularly maintained? Will the device require patches/updates to software to maintain acceptable and safe performance? How will updates be delivered, verified, and are accessories required? • Does the risk assessment consider risk of potential intrusion based on the projected level of cyber security threat during the expected life of the device and identify possible mitigations/strategy during design? • 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?

Essential Principle	Cyber security considerations
6. Benefit of medical devices to outweigh any undesirable effects	• Does the benefit of the device outweigh the residual 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?
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 security vulnerabilities in other devices or other networks? How can risks posed by other devices 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? • Will lack of cyber security 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? • Are appropriate cyber security controls in place to ensure the applicable confidentiality, integrity and availability of information collected by the device? How will a user become aware of any issues with regards to this information?
12. Medical devices connected to or equipped with an energy source	• Can the performance, reliability, and repeatability of the device be affected by cyber vulnerabilities? • Has the device or software been designed and produced, and offer maintenance, having regard to best practice in software and security engineering in order to

Essential Principle	Cyber security considerations
	provide cybersecurity of the device against current and reasonably foreseeable threats? • Does the device include protection against unauthorised access, unauthorised infuence and unauthorised manipulation? • Have risks associated with known cybersecurity vulnerabilities been minimised (through either the remediation of known vulnerabilities and/or the application of the compensating controls)? • Is there a suitable vehicle for informing users of known vulnerabilities in the device and associated mitigations? • Is there a means of applying updates, patches, compensating controls and other improvements, and of supplying sufficient information for a user to make decision with respect to the safety of applying, or not applying them? • 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 programming interfaces?
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? Is the format and structure (free text, structure or machine interpretable) of the information provided appropriate to the expected audience? • Does the device have an expected end of support date for the software and is this communicated? • What cyber security measures, specific to the device, are recommended / required for networks that this device connects to? • Does the information explain to users how to maintain cyber security for the device, how to know if cyber security has been compromised and the steps to take during and after a cyber incident? Is there risk associated with applying security updates?

Essential Principle	Cyber security considerations
	• Does the information include technical details which are necessary for risk management of hospital networks (if applicable)? • 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 for software products and accessories?

Relevant standards

The application of standards is one way to demonstrate that 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 suitable to meet regulatory requirements for cyber security of medical devices, alongside the relevant Essential Principle that may be demonstrated. Alongside relevant standards, other risk management strategies can be adopted if they are generally acknowledged state of the art.

As technology evolves and new standards and guidelines are developed, manufacturers and sponsors will need to be aware of the changing state of the art relevant to their devices. Manufacturers and sponsors are encouraged to review international guidance and publications concerning medical device cyber security, and review established and emerging practices from the broader cyber security sector, many of which have been applied in complex industry environments where risk reduction is a primary focus.

Table 2: Standards recognised as suitable to meet regulatory requirements for cyber security of medical devices, alongside the relevant Essential Principles (EP) (indicates relevant; - indicates 'consider applicability')

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—Requirements for regulatory purposes	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 62304 Medical device software—Software life cycle processes	Defines the life cycle requirements for medical device software: the set of processes, activities, and tasks including development, maintenance, configuration management and problem resolution.	-		-					-		

Standard*	Scope	EP1	EP2	EP3	EP4	EP5	EP6	EP9	EP10	EP12	EP13
IEC 60601 (series) Medical electrical equipment—General requirements for basic safety and essential performance	Widely accepted benchmark for medical electrical equipment. The standards covers safety and performance for electrical medical equipment and helps to ensure that no single electrical, mechanical or functional failure shall pose an unacceptable risk to patients and operators.	-		-	-		-				-
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					-			-		-

Standard*	Scope	EP1	EP2	EP3	EP4	EP5	EP6	EP9	EP10	EP12	EP13
UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	Applies to network-connectable products that shall be evaluated and tested for vulnerabilities, software weaknesses and malware: (i) developer risk management process requirements; (ii) methods to test vulnerabilities, software weaknesses and malware; and (iii) security risk control requirements.					-	-		-		-
UL 2900-2-1 Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems	Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems. It is a security evaluation standard that applies to medical devices, accessories to medical devices and medical device data systems.					-	-		-		-

Standard*	Scope	EP1	EP2	EP3	EP4	EP5	EP6	EP9	EP10	EP12	EP13
IEC 80001 (series) Application of risk management for ITnetworks 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.	-			-	-	-		-		
AAMI TIR 57 Principles for medical device security—risk 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.					-			-		-

Standard*	Scope	EP1	EP2	EP3	EP4	EP5	EP6	EP9	EP10	EP12	EP13
IEC 80002(series) Medical device software	Provides guidance on the application of ISO 14971 to medical device software, methods for validation of software for medical devices 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/IEC 15408 (series) 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 82304-1 Health software—Part 1: 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.										

Standard*	Scope	EP1	EP2	EP3	EP4	EP5	EP6	EP9	EP10	EP12	EP13
ISO/IEC 29147 Information technology — Security techniques — Vulnerability disclosure	Details the methods a vendor should use for the disclosure of potential vulnerabilities in products and online services.		-	-		-	-		-	-	
ISO/IEC 30111 Information technology— security techniques— vulnerability handling process	Explains how to process and resolve potential vulnerability information in a product or online service.								-	-	
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).	-	-	-			-		-	-	

Standard*	Scope	EP1	EP2	EP3	EP4	EP5	EP6	EP9	EP10	EP12	EP13
ISO 14708-1 Implants for surgery -- Active implantable medical devices -- Part 1: General requirements for safety, marking and for information to be provided by the manufacturer	Specified the general requirements for active implantable medical devices and safety requirements including those for electrical, mechanical, thermal, and biocompatibility hazards. The standard is also applicable to some non-implantable parts and accessories				-	-	-		-		
IEC 61010-2-101 Safety requirements for electrical equipment for measurement, control, and laboratory use—Part 2-101: Particular requirements for in vitro diagnostic (IVD) medical equipment	Applies to equipment intended for in vitro diagnostic (IVD) medical purposes, including self-test IVD medical purposes.			-	-	-	-				-

**Use the current version of each standard as appropriate.*

Cyber Security Key Terms

Vulnerabilities

Vulnerabilities are weaknesses 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 vulnerability monitoring (cyber security risk monitoring) or by notification to the manufacturer/sponsor by a third party. When a vulnerability is identified a manufacturer must assess the risk posed to 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 without implementing specific mitigations or patches due to no known active exploitation, a low likelihood of exploitation, or negligible potential risk of harm to patients, this should still 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 in a ‘zero day’ attack. This is an attack that exploits a vulnerability that the vendor or development may be unaware of.

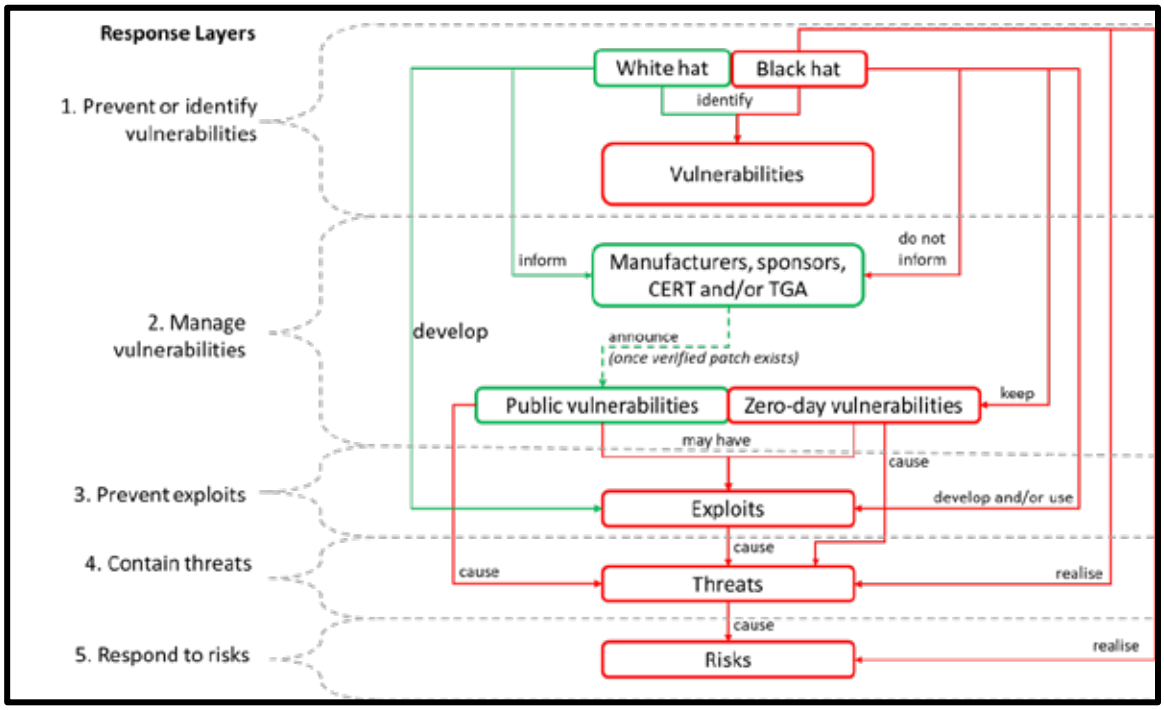
Exploits

An exploit is a piece of code, software or tools that takes advantage of (one or more) vulnerabilities in the software or hardware to gain access to a network or system. Numerous exploits are publicly accessible and are packaged as executables or source code. These exploits may also be packaged into toolsets for improved usability.

Threats

Threats can emerge with the existence of vulnerabilities and adversarial motives to exploit these vulnerabilities—a situation that has the potential to cause harm. For example, the threat on patient privacy, such that data may be exposed to unauthorised individuals; or the threat on patient safety, such that a compromised device may no longer complete its intended task. Black hat adversaries may instigate an attack by strategically using several exploits to realise threats and achieve their objective.

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



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 risks, including cyber security vulnerabilities that may impact the safe operation of their medical device and how these will be addressed.

In order to monitor for vulnerabilities that will affect a given device, the manufacturer should maintain a Software Bill of Materials (SBOM) to better assess risk should a vulnerability be discovered.

Manufacturers should share information with the TGA, (see Post-market guidance), and the wider industry regarding cyber security vulnerabilities that are discovered and threats that emerge.

In a case where cyber security vulnerabilities, threats and risks pose an immediate and significant threat to the health and safety of users or will result in deficiencies or potential deficiencies to the safety, quality, performance or presentation of the device, this information must be shared with the TGA and a corrective and preventative action taken.

Pre-market guidance

Pre-market 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 Principles, the Sponsor needs to demonstrate that cyber security risks have been addressed.

The TGA has a risk-based approach to the regulation of medical devices. The level of scrutiny by the TGA of a device before it is placed on the ARTG and supplied in Australia depends on the risk posed by the device. The lowest risk medical devices, Class 1 devices, are not assessed by the TGA prior to inclusion on the ARTG. For all classes of medical devices, evidence is required to be made available when requested by the TGA to demonstrate that medical device risk, including 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 demonstrate 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. These activities are critical to reduce the likelihood of cybersecurity vulnerability being exploited leading to unacceptable risk to a patient, and for the management of emerging and ongoing cyber security risk and they should be documented in a manufacturer's quality management system.

Alongside the TGA's regulatory requirements for device safety, performance and quality, manufacturers are reminded that some devices may also have other regulatory requirements that need to be met, for example, the Office of the Australian Information Commissioner's Notifiable Data Breach Scheme under the *Privacy Act 1988*.

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. The potential for new cyber security risks that will emerge over the usable life of the device must also be considered and planned for, with upgrade pathways proactively developed where appropriate to address these issues once the device is on the market. Manufacturers should also proactively consider how to reduce risks associated with 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:

- Secure by design: developing 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, such as minimisation of the potential attack surface,

secure code, etc. The Software Assurance Forum for Excellence in Code (SAFECode) publishes information concerning secure software development.[3]

- Quality by design: building on the secure by design approach, quality by design involves understanding and mitigating the potential risks introduced with each function of the medical device, its manufacturing process and the environment in which the device is used. These risks may include cyber security, privacy, usability, safety and other associated risks. While an increase in functions (e.g. Bluetooth connectivity) may lead to improved usability, the way the function is designed, manufactured or used may also increase the device's exposure to cyber security vulnerabilities. More exposure increases the likelihood of a cyber security vulnerability being exploited, leading to potentially unacceptable risks. Early assessment allows for a stronger balance between functionality and cyber security.

Application of standards

The Essential Principles require that design solutions adopted by medical device manufacturers will have 'regard to the generally acknowledged state of the art'[4]. In many instances, this expectation is achieved by the application of standards, some of which are outlined in Relevant Standards. The standards outlined in Table 3 are generally 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 Relevant Standards).

Manufacturers should be mindful that application of standards alone does not guarantee compliance to the Essential Principles. Additionally, application of standards does not guarantee adequate cyber security given the rapidly changing pace of cyber-attacks against the typical timeframes for standards development and implementation.

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—Requirements for regulatory purposes
IEC 62304	Medical device software—Software life cycle processes
IEC 60601 (series)	Medical electrical equipment—General requirements for basic safety and essential performance

[3] Software Assurance Forum for Excellence in Code (SAFECode), Fundamental Practices for Secure Software Development; Essential Elements of a Secure Development Lifecycle Program, Third Edition, March 2018, [Online] Available from: https://safecode.org/wpcontent/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf—Accessed: 10/03/19

[4] Therapeutic Goods (Medical Devices) Regulations 2002, Schedule 1, clause 2(1)—Essential Principle 2(1)

** Use the current version of each standard as appropriate.*

Risk management strategies

Risks that must be managed are detailed in the Essential Principles. Broadly, these include risks associated with the intended use of the device, long term safety, transport and storage, reasonably foreseeable environmental conditions, and unavailability of maintenance and calibration. 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. A separate cyber security risk assessment in addition to the product risk assessment is an acceptable approach.

Two potential strategies to manage risk are detailed below, including the process outlined in ISO 14971 and the USA's National Institute of Standards and Technology's (NIST) cyber security framework. While ISO 14971 is the most commonly applied risk management strategy, others can be used as long as they ensure a manufacturer is adequately assessing, controlling and monitoring risks.

ISO 14971 standard

The ISO 14971 standard specifies a process through which the manufacturer of a medical device can identify hazards associated with a medical device, estimate and evaluate the risks associated with these hazards, control these risks, and monitor the effectiveness of that control.

The following qualitative levels of severity of patient harm, based on descriptions in ISO 14971, could be used in a cyber security risk assessment:

- **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
- **Catastrophic:** Results in patient death

The quantity of patients affected by the risk may warrant an increase in the severity of harm, for example it may be more appropriate to describe a critical level of harm to many patients as catastrophic.

The following summary is provided as an example of a risk management process under ISO 14971[5]:

[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

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 reduced to an acceptable level
7. **Risk control**
   a. Has the cyber security risk been reduced as far as possible or 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?
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.

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 an approach used as a way to address cyber security risks. Originally developed for critical infrastructure, the framework is also beneficial for manufacturers of medical devices and the broader healthcare ecosystem. The framework describes a series of concurrent and continuous cyber security

functions that underpin a cyber security risk management strategy for both pre- and post-market phases[6]:

- **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
- **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.

Management of manufacturing and supply chain

Medical device manufacturers need to consider the cyber security practices of their manufacturing and supply chain, ensuring that relevant components 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 Principle 2: Design and construction of medical devices to conform with safety principles
- Essential Principle 4: Long-term safety
- Essential Principle 5: Medical devices not to be adversely affected by transport or storage
- Essential Principle 9: Construction and environmental properties.

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 and response plans of their suppliers and any platforms that their products will operate on or be distributed through (this includes mobile devices, web services and cloud services). On-going monitoring of practices should also be implemented and manufacturers should act in a timely manner should they discover a cyber security (or other) issue from a component within their supply chain.

Agreements should include expectations about cyber security practices of third parties to ensure the confidentiality, integrity and availability of applicable systems. Where appropriate, thresholds and timelines for supply chain reporting of cyber security incidents should be agreed.

[6] 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

Provision of information for users

Essential Principle 9 requires, among other things, that a medical device manufacturer must 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[7]. To meet this requirement and those of Essential Principle 13 (Information to be provided with medical device), appropriate information on cyber security must be provided to users of medical devices. This should include plain-language information for users with little or no cyber education, and technical language information for those with more advanced understanding. Considerations for cyber security specific information that may need to be provided in line with Essential Principle 13 can be found in Table 1.

Effective communication is required for consumers to understand risk and give informed consent to treatment. This can be a challenge when both the clinician and the consumer may lack specific expertise on medical device cyber security, compounded by the rapidly changing pace of cyber security. Because of this, the requirements for manufacturers to provide clear, high quality and usable information to clinicians and consumers about cyber security risks and how to mitigate them are vitally important.

Clinicians need to be provided with the information to have a meaningful discussion with the patient about the risks and benefits of a particular device they are prescribing, including cyber security risk. This information needs to be in a language that is relevant to them, and their patients. In the case of high risk devices, clinicians must also have access to information to understand how and when to apply an update to a device.

Provision of information is also important for consumer focused medical devices, 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.

As healthcare service providers increasingly strive to create a cyber secure environment, medical device manufacturers and sponsors supplying to these service providers will be asked for more specific information on cyber security risk mitigation measures during procurement activities. Collaboration between these organisations is essential to creating a more cyber secure healthcare environment. The USA's National Electrical Manufacturers Association (NEMA) provides an example form that manufacturers might consider when providing information to healthcare services providers (see *Manufacturer Disclosure Statement for Medical Device Security*). Further, a list of potential questions suggested for procurement teams are listed in the TGA's medical device cyber security guidance for users of medical devices. These 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 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., development environment, build tools, and the supply chain)?

[7] Essential Principle 9.2(b)

- Does the manufacturer/sponsor provide an ongoing service to manage the security of the medical device(s), and how will they respond to future cyber security incidents?
- A medical device often has a long lifecycle—does the manufacturer/sponsor 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?
- Has the company experienced any cyber security issues over the past 12 months and how were these managed?

Technical cyber security considerations

There are a number of technical cyber security considerations that a manufacturer should address during the pre-market development of a medical device to help ensure that cyber security risks to patient safety are designed out, removed, eliminated, reduced or otherwise managed. A number of these considerations are detailed here; however, manufacturers should be aware that technical considerations will vary depending on the device in question, the intended use, and the environment of use. Refer to *ACSC (Australian Cyber Security Centre),* and in particular, the "Essential Eight" baseline mitigation strategies to protect against cyber threats.

Modularised design architecture

- It is best practice to modularise or partition aspects of the design architecture to enable independent function of modules for cyber security.
- 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.
- A secure operating platform, such as a security-verified microkernel, verifies the design architecture and enforces component separation in the designed partitions in order to prevent a critical software component from being negatively affected by other software components and cyber security attacks targeting them.
- Smaller components are easier to assess for cyber resilience, by application of methods including formal mathematical proofs. Reuse of validated or verified trustworthy modules in different devices will improve overall cyber security, with reduced effort.

Cyber security assessment and penetration testing

- Consider implementing penetration testing initiatives (commensurate with risk level) to validate the effectiveness of medical device cyber security measures and internal risk management practices, and identify unknown vulnerabilities:
  - 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.
  - Cyber security performance testing should be performed by a qualified party independent of the development team. Collaboration or partnership with 'white-hat' hackers, biomedical engineering teams and cyber security professionals is recommended.

  - Utilise information from recognised organisations and industry groups regarding application security risks. One example of an accessible source is the Open Web Application Security Project which provides a list of the Top 10 most serious web application security risks each year.
  - 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. Network threat modelling using approaches such as the MITRE ATT&CK framework are also recommended to improve the cyber resilience of devices.[8]

- Regular code review and penetration testing should cover assessment of common cyber security vulnerabilities (like the examples in Appendix 1: Known vulnerabilities) through database checks, use of known exploits and tools like vulnerability scanners, or software behaviour analysis using specific scenarios. Cyber security risks that should be assessed include:
  - Insufficient use of appropriate encryption and authentication protocols
  - 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, open JTAG ports
  - Improper use of control statements, e.g. improper checks for unusual or exceptional conditions
  - Wrong implementation of algorithms and protocols, e.g. OpenSSL's 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 APIs
  - Lack of input sanitation and data validation, e.g. allowing potential injection attacks
  - Checking potential vulnerabilities through control flow analysis or fuzzing
- Take action on outcomes of penetration testing by assessing the risk(s) of the affected functions, and consider solutions that address the risk(s) according to Essential Principle 2.
- Continual assessment of the threat landscape and up-to-date intelligence on new and emerging vulnerabilities is vital to cyber security assessment.

[8] Storm, B., Battaglia, J., Kemmerer, M., et al (2017). *Finding Cyber Threats with ATT&CK™-Based Analytics*, MITRE Corporation, [Online] Available from: https://www.mitre.org/sites/default/files/publications/163713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf Accessed: 13/03/2019

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 (EPs), in particular EP 2 (Design and construction of medical devices to confirm with safety principles), EP 3 (Medical devices to be suitable for intended purpose) and EP 9 (Construction and environmental properties).
  - This is particularly critical for software development where the product is intended to operate on a consumer mobile device, or utilise a web or cloud service. It is required that the manufacturer or sponsor will have assessed the cyber security risks introduced by the third party platform and inform the user where there is residual risk, in order to meet the requirements of the Essential Principles.
- High-level considerations include the cyber security protections and support that a third party provides for its platform (covering differential responsibilities, processes and risks specific to the medical device domain), 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 may indicate that the firmware is from an unauthorised (potentially malicious) source or that the firmware code has been tampered with.

Update pathways

- Manufacturers must consider the risks associated with available update methods and pathways, whether manual, remote access, continual updating using cloud/virtual systems, or another approach. Additionally, manufacturers must consider the ability for secure updating of a medical device during its lifecycle to account for emerging cyber risks, and demonstrate that the approach is in alignment with current state of the art practice.

Trusted access and content provision

- Manufacturers and sponsors are encouraged to implement trusted access measures for network connected devices to prevent unauthorised access and to reduce cyber security risk. This should focus on securing activities that will be undertaken by the medical device user and ensuring the device can only access networks that are absolutely necessary. Measures manufacturers should consider include:
  - Consider both physical and network access requirements—this might include removal of internet accessibility and direct network connectivity where appropriate and physically locking a device
  - Incorporate Multi-Factor Authentication (MFA), which uses two or more authentication factors to confirm the user's identity. MFAcan limit the consequences of a compromise by preventing or slowing an adversary's ability to gain unrestricted access to an asset.

  - Build in best practice access requirements (e.g. password, biometric, smartcard), account lockout protocols, and automatic timed methods to terminate sessions where appropriate.
  - Establish, collect, and analyse logs to ensure traceable activity on the device and ensure trusted and credentialed access
  - Utilise user profiles (restrict administrative privileges) that limit device access and privileges, balancing access and security (role-based access), and regularly revalidate the need for given privileges.
  - Establish an incident response plan in a case of any malicious activity.
- Encryption of medical device data is recommended, both at rest and in transit, where appropriate. Encryption refers to the conversion of original information/plaintext data into incomprehensible text known as ciphertext using an encryption algorithm. The use of encryption protects patient health information when it is transmitted from one user to another.
- Manufacturers need to ensure that, as far as practicable, risks associated with the foreseeable environmental conditions are minimised which includes security risks of the networks on which a medical device is intended to operate on (Essential Principle 9 Construction and environmental properties—see Table 1).

Refer to the ACSC (Australian Cyber Security Centre) website for more details.

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. This means that risks identified on cyber.gov.au will also be considered as representative of the current risk environment.

Evidence of compliance with the Essential Principles, and other legislation, must be supplied to the TGA if requested.

The inclusion of a 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[9]. Breaching the conditions of the inclusion of a medical device may lead to suspension or cancellation of the entry for that device from the ARTG[10], may be an offence[11], and may contravene a civil penalty provision[12].

Consistent 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

[9] See subsection 41FN(3) of the *Therapeutic Goods Act 1989*
[10] See Part 4-6 of Chapter 4 of the *Therapeutic Goods Act 1989*
[11] See subsections 41MN(1), (4) and (4A) of the *Therapeutic Goods Act 1989*
[12] See subsection 41MNA(1)) of the *Therapeutic Goods Act 1989*

quality management systems must be updated appropriately over the life cycle of a device to maintain inclusion on the ARTG. It is critical that the change management process, e.g. as outlined in IEC 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.

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

   iv. 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 (e.g. ISO 14971, NIST cyber security framework) and is a re-occurring activity. As with other risks, the changing nature of cyber security risks means that it cannot be mitigated through premarket controls alone, and requires ongoing management. Cyber-security risk monitoring and management needs to be an integral aspect of the post-market monitoring activities conducted by a manufacturer and sponsor(s).

Cyber security is an ongoing activity.

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 high-level 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 be unintentional.

Further, insider threats present a challenge to both manufacturers and users of medical devices. Employees, contractors or partners wishing to cause harm represent a significant source of threat. Having authorised access allows insiders to potentially compromise confidentiality, integrity or availability of medical devices and their networks and data. Malicious or accidental insider access to a device or deletion, alteration, falsification, or unauthorised sharing of patient data is a real challenge that manufacturers need to be aware of, identify and address.

Cyber security 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 or 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 and as part of a sponsor's post-market obligations, ongoing monitoring and surveillance of safety and performance is required, including monitoring for cyber security issues. This approach to monitoring cyber security intelligence and information should be clearly outlined during the development of the medical device. 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(s) (through adverse event reports, complaints, and monitoring of CERT alerts)
- TGA (through post-market monitoring and compliance activities)
- other regulators, who may notify the TGA
- a Cyber Security Operations Centre or Security Information and Event Management capability, either internal to the organisation or as a service provider
- 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)

In order to monitor for vulnerabilities that may affect a given device, the manufacturer should maintain a Software Bill of Materials (SBOM) to cross-reference for improved assessment of risk should a vulnerability be discovered. If a cyber security vulnerability is identified through monitoring activities, the manufacturer should work with the source (where appropriate) to understand the issue and conduct a risk assessment. 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 threat information sharing is an important component for a safe and secure digital ecosystem. Such an information sharing system provides parties along the supply chain, but especially the manufacturer and sponsor, with the capability to identify threats, assess associated risks, and share best practice approaches to addressing these. Information empowers organisations with knowledge to monitor threats and respond accordingly.

In Australia, general cyber security threat information sharing and monitoring can be facilitated through CERT Australia (as part of the Australian Cyber Security Centre). Other Australian options for medical device organisations to formally share information on cyber security threats are currently limited; however, the TGA encourages informal networks of manufacturers to share information on threats and recognises the value of information from international organisations (e.g. health focused Information Sharing and Analysis Organizations (ISAOs) in the USA).

Risk assessment

A manufacturer 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 succeeding 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 if the vulnerability were to be exploited (Figure 2)[13] Manufacturers/sponsors should have a process for assessing the severity of patient harm should the cyber security vulnerability be exploited. For example, the qualitative severity levels of patient harm, as described in ISO 14971.

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 where there is a low risk to the intended benefit or unacceptable, with a high risk to intended benefit.

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 ISO 14971) 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. Risk assessment should be a re-occurring activity with a frequency based on the level of risk and any new information that is uncovered.

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

- Where a medical device is identified as having deficiencies or potential deficiencies to the safety, quality, performance or presentation due to a cyber security vulnerability 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.
- Where residual risk is acceptable, sponsors and manufacturers are required to proactively promote practices that continue to reduce cyber security risks. In such circumstances, consideration could be given to initiating a non-recall action if the medical device meets all specifications/standards and no deficiencies exist in safety, quality, performance or presentation.

Updates and change control

Manufacturers are required to assess which course of action to take prior to making updates to medical devices (including to software). Such a proposed change may require an associated recall action, e.g., a safety alert, routine update, submission of an adverse event report, or a device recall.

Changes to software that do not have implications for safety, quality, performance or presentation generally do not require any form of recall action; however, the manufacturer should consider whether its certifying body should be notified of the change.

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

Manufacturers and sponsors are required to update risk management systems following the rollout of updates to medical devices.

[13] 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.

Uniform recall procedure for therapeutic goods (URPTG)

Consult the Uniform Recall Procedure for Therapeutic Goods (URPTG) and follow this procedure as applicable.

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 or public health**. Cyber security issues may also indicate that there has been actual or potential product tampering. In these cases, devices may require an immediate recall. If such a threat is found, sponsors must:

- Consult the 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 Uniform Recall Procedure for Therapeutic Goods and follow this procedure as applicable.

Sponsors must check whether the issue with the therapeutic good(s) requires a recall before considering a non-recall action. Sponsors must decide the type, class and level of recall.

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 are outlined below, as per the URPTG.

Examples of types of cyber security recall actions

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 (to be determined in consultation with the TGA).
- **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.

Examples of class of cyber security recall action

Recall actions related to cyber security could be class I, II or III.

- **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.

Examples of non-recall actions related to cyber security

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 for commonly used accessories, or networks that the device uses, become 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.

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:

- **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.

Cyber security intelligence and threat sharing

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.

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

- 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

Manufacturers and sponsors

Manufacturers and sponsors must demonstrate how they will gather information regarding emerging cyber security vulnerabilities that may impact the safe operation of their medical device, and demonstrate assessment and any relevant action as part of ongoing risk management. This is necessary to ensure that a medical device included in the ARTG continues to meet the requirements of the Essential Principles.

This can be achieved by ensuring that complaint monitoring processes for manufacturers and sponsors includes cyber security issues. Manufacturers and sponsors are encouraged to:

- monitor threat-sharing websites or join informal intelligence sharing groups

- share information with the TGA and the wider industry regarding cyber security vulnerabilities and threats that they discover

Appendix 1: Known vulnerabilities

The following list, which is not exhaustive, contains examples of known cyber security vulnerabilities for medical devices.

1. Authentication bypass
2. Buffer overflow
3. Code injection
4. Communication protocol vulnerability
5. Credentials insufficiently protected
6. Cross-site scripting
7. Cryptographic issues
8. Data authenticity insufficiently verified
9. Debug service enabled by default
10. Default password
11. Exposed dangerous method or function
12. Flash memory content insufficiently protected
13. Hard-coded credentials
14. Improper access control
15. Improper authentication
16. Improper authorisation
17. Improper certificate validation
18. Improper control of generation code
19. Improper exception handling
20. Improper input validation
21. Improper restriction of communication channel to intended endpoints
22. Improper restriction of operations within the bounds of a memory buffer
23. Power consumption: improper restriction
24. Reference information exposure
25. Leftover debug code
26. Man-in-the-middle
27. Meltdown, Spectre and Spoiler
28. Missing confidentiality
29. Numeric errors
30. Out-of-bounds read

31. Path traversal
32. PC operating system vulnerabilities
33. Protection mechanism failure
34. Relative path traversal
35. Resource consumption uncontrolled
36. Resource management errors
37. Search path element uncontrolled
38. Session expiration insufficient
39. Unquoted search path or element
40. Untrusted input accepted
41. Vulnerable third-party software
42. Weak password hashing algorithm
43. XML external entity: improper restriction

Appendix 2: The evolving cyber security landscape

The TGA is responsible for the continued safety, quality and performance of medical devices affected by cyber-related issues.

Cyber security in Australia

The Australian Government released Australia's Cyber Security Strategy in 2016. This strategy recognises that improving cyber security is a whole-of-economy challenge, and details priority actions to improve Australia's general cyber security posture, alongside supporting the growth of the local cyber security industry.

Putting the cyber security strategy 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).

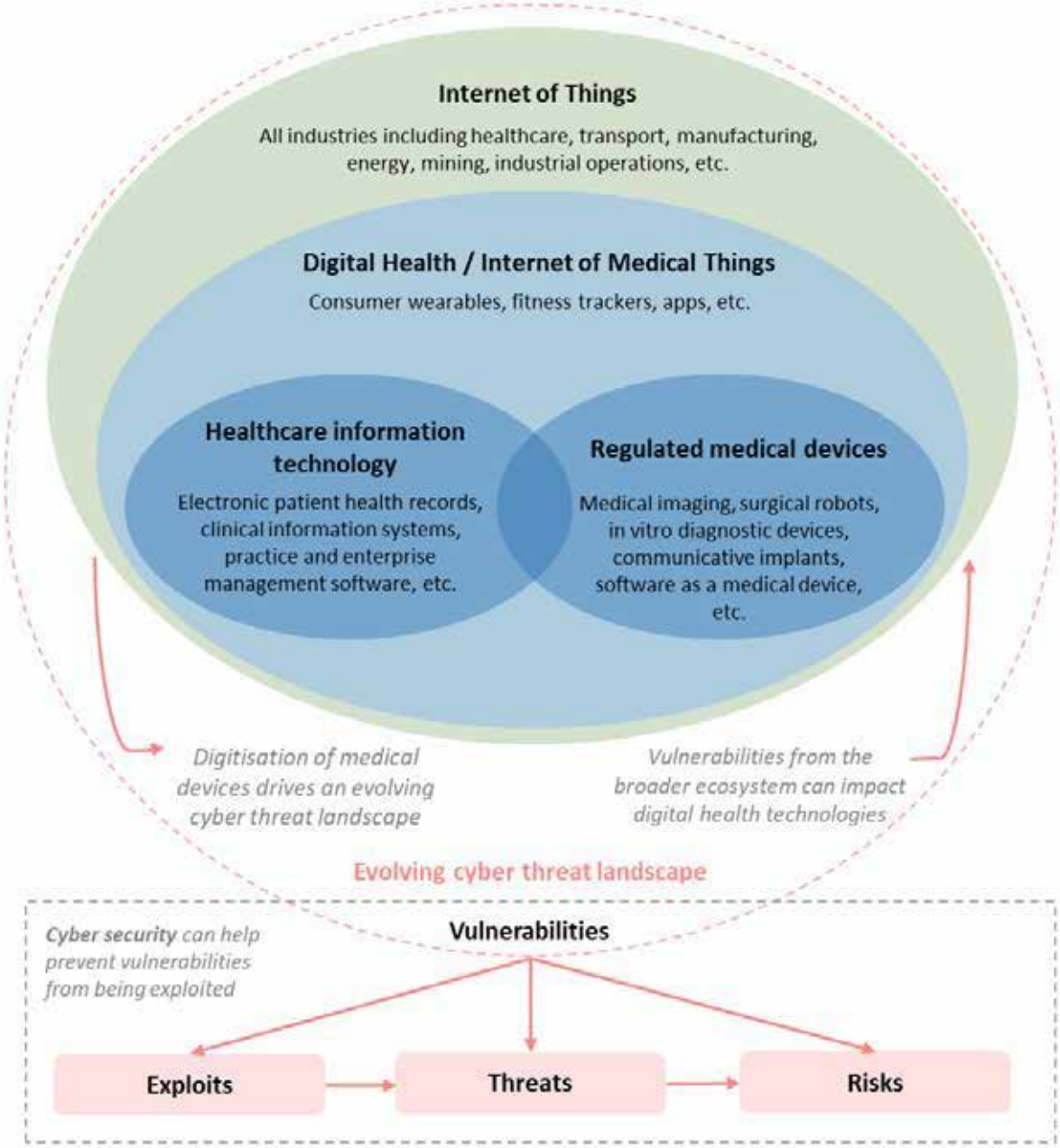
Health technology and cyber security

The digitalisation of consumer and professional health technology 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.

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

Figure 2: The evolving digital health and cyber landscapes



The role of the TGA

As technology progresses, the capabilities and functionality of medical devices are becoming more digitised and interconnected. Software in particular is becoming increasingly important and pervasive in healthcare. As the digital complexity of devices increases so does the potential for cyber security risk through hardware and software vulnerabilities and increased exposure to network and internet-based threats.

In order to support Australia's medical device cyber security capability, the TGA has produced cyber security guidance for industry as well as guidance for users to embed cyber security practices and protocols across the medical device sector (developers, manufacturers, sponsors, health professionals and patients).

Please note that TGA requirements may not be the only relevant regulatory requirements. For example, you might be required to use the Office of the Australian Information Commissioner's Notifiable Data Breach Scheme under the *Privacy Act 1988*.

Manufacturer and sponsor responsibilities

Manufacturers and sponsors need to consider and plan for an evolving cyber security landscape in order to maintain patient safety. 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.
- Digitalisation is blurring the distinction between medical devices and consumer devices, with smartphones able to act as the operating 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.

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.

Motivations for malicious activity

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.
- Generating wide-scale disruption of services by gaining entry into hospital networks
- Alteration or removal of a medical service or therapy to impact lives as a form of cyberwarfare, or to target 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 identify and/or exploit vulnerabilities in complex systems

Industry trends and cyber security considerations

Highlighted below are emerging social and technological trends that are affecting the cyber threat landscape and associated implications for the healthcare and medical device industry. The cyber security effect that arises from each trend is an important consideration for all stakeholders in the healthcare and medical device industry.

Table 4: Healthcare and medical technology industry trends and cyber security considerations

Trend name	Trend observations	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, refer to *ACSC (Australian Cyber Security Centre)* 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	• 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 Ensure clear ownership of responsibilities

Trend name	Trend observations	Cyber security considerations
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, refer to *ACSC (Australian Cyber Security Centre)*
Large-Scale Device Networking	• Wireless communications such as Bluetooth are used in many medical devices which reduces the need for cabling and isolation • Although Bluetooth technology can help the healthcare facilities to improve operational efficiencies it can pose cybersecurity vulnerabilities	• Wireless communications provide an extra surface for cyber attacks, including remote attacks • Security measures should be in place for medical devices with Bluetooth technology, i.e. files can be encrypted before transmitting between devices, or Bluetooth can be turned off when it is not in use. refer to *ACSC (Australian Cyber Security Centre)*
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 name	Trend observations	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	• Manufacturers will need to ensure that confidentiality and integrity of data is maintained
Healthcare: a vulnerable industry	• Healthcare is vulnerable to cyber threats, with many poorly protected legacy systems in use • A legacy medical device is one that likely cannot be reasonably protected against current cybersecurity threats. A legacy medical device is likely to be at the 'End of Support' life cycle stage, where the manufacturer has terminated all service support activities, but may still have clinical utility that exceeds the devices supportability. • Cyber-attacks on healthcare organisations are increasing • Healthcare is vulnerable to mass media communications that can cause a crisis of confidence in health services and products	• Adversaries can have numerous motivations to attack medical devices • Health care organisations should have the facility to identify the legacy systems to be able to isolate them through applying strict access control, refer to *ACSC (Australian Cyber Security Centre)* If a device has reached end of support the cybersecurity exposure will be greater because the original supplier is no longer providing support or security updates. • Healthcare information is highly sought after on the dark web • Manufacturers of devices that capture, transmit or store health information should address the risks created by poor cyber security • Public trust is difficult to restore after a significant cyber event

Appendix 3: Frameworks and standards related to cyber security from other sectors

The rapid change of pace of the cyber security threat landscape relative to the development and implementation of standards means that manufacturers, sponsors and in some circumstances, users of medical devices, must continually assess and understand emerging global cyber security standards and frameworks that are being applied across other industries. This might include defence and financial services where infrastructure security and information confidentiality and integrity are primary drivers. It may also include the Internet of Things community within which connected medical devices are implicitly included, especially consumer devices.

The tables below provide a non-exhaustive 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.

Internet of things (IoT)

Organisation, year	Name of Document	Summary
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) (NISTIR 8200)	Covers connected vehicles, consumer IoT, Health IoT, smart buildings, smart manufacturing Looks at cybersecurity risks as well as standards

Industrial control systems (ICS)

Organisation, year	Name of Document	Summary
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

Organisation, year	Name of Document	Summary
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 Defence-in-Depth Strategies	Strategies for defence and recommendations for securing ICS

Financial services

Organisation, year	Name of Document	Summary
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

Organisation, year	Name of Document	Summary
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 4: International guidance on medical device cyber security

The TGA aims to harmonise where appropriate with relevant international guidance. Many international jurisdictions will have regulatory guidance and information that is in line with global best practice concerning cyber security quality management and risk management systems, and therefore broadly in line with the expectations of the Essential Principles. Ideally, this facilitates the import and export of medical devices to and from Australia.

There are a number of guidance documents on the cyber security of medical devices that have been published or are under development by international medical device regulators. Some of these are discussed below. This is not an exhaustive list of global guidance materials. Meeting the regulatory requirements of one jurisdiction does not automatically mean compliance with the Essential Principles.

For a medical device to comply with the Essential Principles, the TGA requires that the design and construction will conform with generally acknowledged state of the art safety principles, including quality management and risk management systems.

USA guidance

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
- Postmarket Management of Cybersecurity in Medical Devices
- Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices
- Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software
- Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices

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 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

IMDRF guidance

The International Medical Device Regulators Forum (IMDRF) has worked to further a unanimous understanding of challenging topic areas, such as Software as a Medical Device (SaMD), 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
- Software as a Medical Device (SaMD): Possible Framework for Risk Categorization and Corresponding Considerations
- Software as a Medical Device (SaMD): Application of Quality Management System
- Software as a Medical Device (SaMD): Clinical Evaluation

European guidance

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 Internet of Things (IoT):

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

Other jurisdictions

Cyber security for medical devices is a growing area of focus across many other jurisdictions. In some of these jurisdictions, authorities external to country's health departments are investigating cyber security approaches for a range of Internet of Things devices, including connected medical devices. Examples of guidance are highlighted below. Note that some of these are draft, and the fast moving nature of this topic means that there are many jurisdictions and examples of guidance not included here:

- 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.
- The Singapore Standards Council technical reference on Connected medical device security
- Health Canada's draft guidance document on the Pre-market requirements for medical device cyber security

Glossary

The glossary for this guidance is included in the TGA glossary <https://www.tga.gov.au/acronyms-glossary>.

Version history

Version	Description of change	Author	Effective date
V1.0	Original publication	Medical Devices Branch	July 2019
V1.1	Additional advice on revised Essential Principles	Medical Device Surveillance Branch	March 2021
V1.2	Changes to further align with the *Australian Cyber Security Centre*	Medical Devices Surveillance Branch	November 2022

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

医课汇
公众号
专业医疗器械资讯平台
WECHAT OF
HLONGMED

hlongmed.com
医疗器械咨询服务
MEDICAL DEVICE
CONSULTING
SERVICES

医课培训平台
医疗器械任职培训
WEB TRAINING
CENTER

医械宝
医疗器械知识平台
KNOWLEDG
ECENTEROF
MEDICAL DEVICE

MDCPP.COM
医械云专业平台
KNOWLEDG
ECENTEROF MEDICAL
DEVICE