Standard*	Scope	EP1	EP2	EP3	EP4	EP5	EP6	EP9	EP10	EP12	EP13
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.	✓	✓	✓	✓	-	-	✓	-	✓	-
IEC 80001 (series) Application of risk management for IT-networks incorporating medical devices	80001 series of standards define roles, responsibilities and activities for risk management of IT-networks incorporating medical devices. Focus is on safety, effectiveness, data security and system security.	✓	✓	✓	-	-	-	✓	-	-	✓
AAMI/UL 2800 Safety and security requirements of interoperable medical systems	Defines safety specifications that a medical devices interface should be labelled in order to operate in safe conditions. Focuses on risks associated with interoperability within the integrated clinical environment.	-	✓	✓	-	-	-	✓	-	✓	✓

Standard*	Scope	EP1	EP2	EP3	EP4	EP5	EP6	EP9	EP10	EP12	EP13
AAMI TIR 57 Principles for medical device 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.	✓	✓	✓	✓	-	✓	✓	-	✓	-
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.*

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

** 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

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

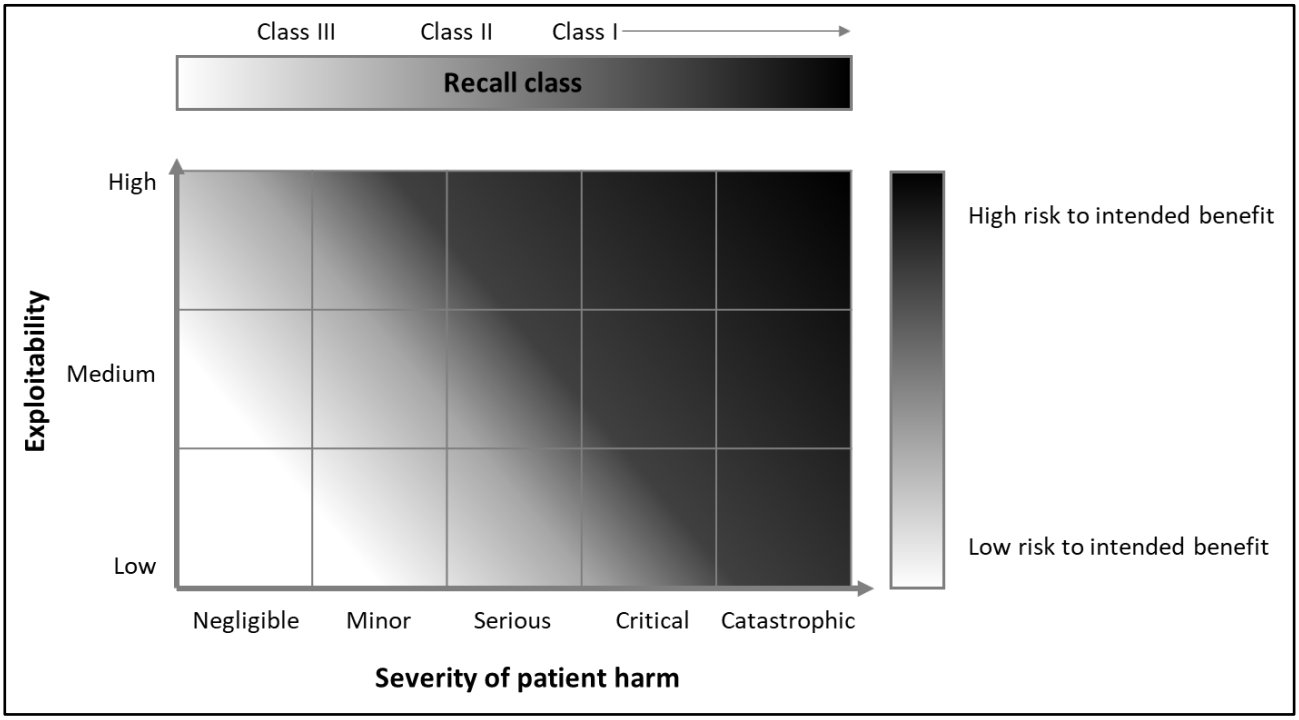
A manufacturer or sponsor's assessment of the risk of patient harm posed by a cyber security hazard that impacts the safety, quality, performance or presentation of a device should consider:

- 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)[12]
  - 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 (Figure 2).

[12] 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.

Figure 2: Evaluation of risk of patient harm



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

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.

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).

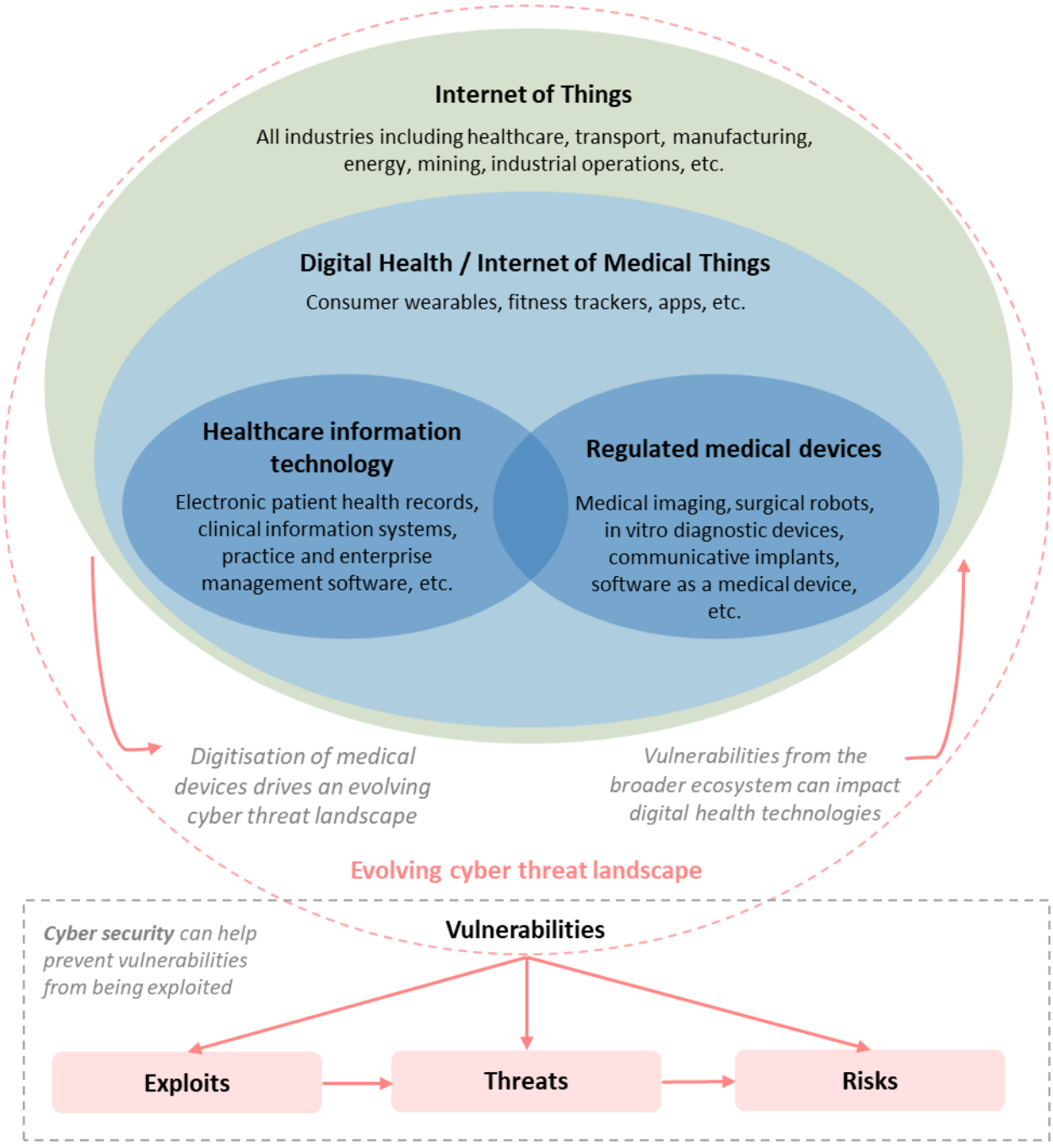
Health technology and cyber security

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.

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 this 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.

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 • 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
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

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

D19-5302505