Australian Government
Department of Health and Aged Care
Therapeutic Goods Administration

Medical device cyber security information for users

Consumers, health professionals, small business operators and large scale service providers

Version 1.2, November 2022

Contents

Introduction

This guidance is intended for groups or individuals who represent users of medical devices including in-vitro diagnostic medical devices (IVDs), such as:

- consumers who use a medical device that does not require medical supervision
- consumers who use a medical device in the ARTG under the guidance of a health or medical professional
- health professionals who use medical devices to diagnose and treat patients
- clinical and biomedical engineers who are responsible for managing medical device assets in a health and medical environment
- healthcare and IT administrators responsible for systems, procedures and processes in a health and medical service environment

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

The TGA recommends that users of medical devices consult cyber.gov.au to see the latest advice and information on cyber security from the Australian government.

Connectivity and digitisation increase benefits and risks

Connectivity and digitisation of medical device technologies may help improve or increase device functionality and provide therapeutic 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 so that it can cause patient harm
- loss of privacy or alteration of personal health data

Cyber security for medical devices must be considered as part of a layered, holistic security ecosystem. The cyber security landscape is constantly evolving.

Software in particular is becoming increasingly important and pervasive in healthcare. As the complexity and interconnectedness of devices increases so does the potential for cyber security risk through hardware and software vulnerabilities and increased exposure to external threats, including via the internet.

Purpose and scope of this guidance

The TGA does not regulate users of medical devices; however, having cyber secure medical devices relies on device users as well as manufacturers and sponsors.

Generally, medical device operating environments are highly variable and cyber security risks are dependent on the knowledge and approach of those who use medical devices. Users of medical devices have a shared responsibility for providing a cyber secure environment for these devices to operate in. While supplying a compliant medical device is the responsibility of the manufacturer and sponsor, a compliant medical device will only be as secure as the most vulnerable aspect of the system it is expected to operate in.

In order to support Australia's medical device cyber security capability, the TGA has produced this guidance to highlight cyber security practices and protocols for the medical

device sector. This guidance will assist medical device users in managing cyber security risk, and helps to supports the Australian Government's cyber security strategy.

Report potential cyber security issues

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

If a medical device appears to have been impacted by a cyber security issue and could directly impact health and safety, users should report this:

- as soon as possible to their health professional (when applicable)
- directly to the TGA by phoning 1800 809 361

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

Guidance for different users

This guidance is structured to consider different groups of medical device users, as:

- Guidance for patients and consumers
  - who use a medical device as directed by a health professional
  - who use a medical device (such as a downloaded software 'app') without professional supervision
  - who might access software that acts as a medical device (e.g. by diagnosing a heart murmur) from overseas websites, even though such software products may not have been approved for use in Australia by the TGA[1].
- Guidance for health and medical professionals
  - who are responsible for the use of medical devices for a range of purposes—described as 'to diagnose, prevent, monitor, treat or alleviate disease or injury in a patient' in the *Therapeutic Goods Act 1989*
  - which includes medical doctors, nurses, radiologists and radiographers, pathologists, etc.
  - who may be based in a medium to large health or medical organisation such as public hospitals, private health service providers
  - who may be able to access, review and exchange data with devices, and may also be responsible for patient education and establishing parameters for how devices and software are to be used
- Guidance for small business operators (including small-practice clinicians)

[1] Note that use of unapproved medical device software is not recommended.

  - who are responsible for the procurement, implementation, maintenance, and application of medical devices in a small clinic environment or general medical practice
  - who are generally reliant on information provided by the manufacturer or sponsor regarding medical device cyber security
  - who may not have the ability to detect potential cyber security problems themselves
- Guidance for large scale service providers with specialist teams
  - who are responsible for the procurement, implementation and maintenance of medical devices in a health and medical service environment, such as a hospital
  - which includes biomedical engineers and IT experts who have the task of ensuring continuous operation of health services
  - who are likely to have cyber security related knowledge and may also have related expertise

Guidance for patients and consumers

Patients and consumers using connected medical devices should:

- be fully informed about the potential cyber security risks these devices may expose them to
- take proactive action to protect their devices and networks, and act responsibly online

Consumer information, which includes basic security advice for medical devices, is available.

When receiving a medical device that has risks associated with cyber security, it is important that consumers are able to understand this risk and associated benefits in order to give informed consent. Alongside receiving information on the device, consumers are encouraged to ask their health professional questions to help build their understanding of using the device safely and securely. These questions might include:

- What are the risks, particularly cyber security risks, associated with use of a specific device and what alternative device options exist? What constitutes a cyber security risk?
- What default security settings are there to protect the user?
- What are the cyber security implications of changes to the device settings?
- When and how does the device connect to the internet?
- What data is collected by the device, where does it go, and who has access to it?
- How can a user tell if a device has been hacked or compromised and who can they talk to if this is suspected?
- Who should the user talk to if they learn about vulnerabilities (e.g. from the media or TGA) that might affect the device?
- What does the user need to do to maintain the device (e.g. software updates)?

The Australian Cyber Security Centre provides guidance to consumers and small business operators to help reduce cyber security risk associated with software vulnerabilities, online scams, malicious activities and online behaviours. This is important for:

- maintaining the operating integrity of a medical device so that it may continue to deliver its intended therapeutic benefit
- assisting in maintaining the confidentiality, integrity and availability of medical devices and their data
- creating a cyber safe operating environment for connected medical devices

Privacy

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

- Some digital health products (e.g. medical software apps) may provide a forum for users to interact. However, asking specific questions and sharing of information that can lead to personal identification should be carefully considered.

Passphrases

To provide maximum security of information, the Australian Government recommends[2] users choose strong (long, complex, unpredictable and unique) phrases (a phrase made up of at least 14 characters ideally four or more words) over other types of passwords when setting up devices and accounts or updating their log in details. Passphrases can be used when multi-factor authentication is not available. Multi-factor authentication should be used when available. When creating and using passphrases, best practice is to:

- Avoid reusing the same passphrase across different services especially if they are registered under the same email address.
- Never share your passphrases with anyone
- Be aware of your surroundings when using log in details in public.
- Only use trusted connections, or a Virtual Private Network (VPN) when accessing an account, as using public Wi-Fi, without the use of a VPN, increases the risk that your information could become compromised.

Refer to Creating Strong Passphrases on the ACSC website: www.cyber.gov.au for more details.

- Many connected medical devices will require an account to be created, either in a companion app or an associated online platform. It is recommended that strong passphrases be used to protect these accounts, their associated information and any control that unauthorised access may allow.

Suspicious messaging

Treat any unexpected messages with caution.

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

[2] https://www.staysmartonline.gov.au/Protect-yourself/Doing-things-safely/Passwords-passphrases

sponsor or medical professional, don't use the details or any links in the suspicious message, use contact details that you trust.

Online health and medical details

Similar to online banking details, criminals are eager to steal personally identifiable health information. Users should ensure that connected devices—including computers, mobile devices, and medical devices—comply with the operating instructions provided with a medical device. Refer to "Guidelines for System Hardening" on the ACSC website: www.cyber.gov.au for more details.

Tablets and mobiles

These days tablets and mobile phones are often an accessory to a medical device. For example, a medical device may have a phone app that assists in using the device or collecting data. In these cases the security of the phone or tablet can directly affect the security of the medical device.

Users should turn on the security features of their mobile devices, set a password/phrase or PIN that must be entered to unlock the device, install reputable security software and ensure they are using the most up-to-date operating systems. Refer to guides on "Mobiles and Tablets" on the ACSC website: www.cyber.gov.au for more details.

Backups and updates

Regularly updating applications (e.g. phone apps and operating systems) associated with medical devices is important because the most up-to-date software will generally be the most secure.

Users can reasonably expect that manufacturers will provide security updates, disclose known vulnerabilities and make available sufficient information for a user to discuss with their health care professional and decide whether to apply or not apply updates and other improvements.

Medical devices may be attacked through the networks they are connected to, some of which are home networks (e.g. home WiFi or internet). Therefore, updating security software for your home networks and IT equipment is also important for protecting your medical devices. Users should make sure their computers are secure and up-to-date and should regularly update the firmware within their routers and modems, or turn on automatic updates.

As with other data and systems, backups are important so that, in the worst case, the system can be recovered and restarted. Data and settings collected by medical devices can be critical to a user's health care, so users should make sure that this data is backed up with their other critical data.

Using smart devices in the home

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

- Whenever possible, change any default passwords on the device to a secure and private passphrase.

  - Medical devices often come with default passwords so that doctors and consumers can start the device after buying it. However, these passwords are known by others and may be easily guessed.

- When practical and safe, ensure software updates are set to apply automatically on any devices.
  - Special consideration should be given for medical devices because updating them can affect the medical care that the devices provide. Check with your doctor about automatically updating your medical devices or their accessories.
- Follow all instructions when installing and configuring the settings for the device.
  - Patients and consumers using connected medical devices should always read and understand the information provided with the medical device, including its intended purpose and any limitations of use, the instructions for maintenance and use of the device, and how updates are to be provided for the device (e.g. software and firmware updates). Patients and consumers should also talk to their clinician if they have any questions about the instructions.
- Continue to be vigilant about protecting devices throughout their lifespan.
- When using connected medical devices outside the home, users should exercise caution, especially if using public wireless networks or internet 'hotspots' that are run by organisations that are not trusted, and avoid sending or receiving sensitive information while connected to public networks.
  - Consider that attackers also have easy access to public networks. This means that information can be easier to intercept and you have one less layer for securely protecting your medical device.

Guidance for health and medical professionals

Health and medical professionals use medical devices to diagnose, prevent, monitor, or treat their patients. Alongside understanding the clinical benefit of the device, health and medical professionals have a responsibility to:

- **report any potential cyber security issues with medical devices to the TGA directly by phoning 1800 809 361**
- pass on relevant cyber security risk information associated with use of the device to the patient
- communicate benefits and risks of using the medical device to the patient, such that they are suitably informed to provide consent
- upskill themselves on the safe and secure use of the medical device, where the device is a common tool used by the professional for delivery of healthcare
- act on any advice from the TGA, the device manufacturer or sponsor in the event that a cyber security vulnerability or risk is disclosed

Getting the right information

Health and medical professionals need to become familiar with the cyber security risks associated with medical devices they prescribe, implant or use. Information regarding cyber security risks is provided with the medical device by the manufacturer. If more information is required, health professionals are encouraged to ask the manufacturer questions to ensure

they understand any associated cyber security risks. Health and medical professionals should understand the following:

- clinical and cyber security risk associated with use of the device
- how security of the device must be maintained
- what they must do in the event of a suspected cyber security breach
- what they must do in the event of a suspected cyber security vulnerability

In a hospital setting, health professionals may be able to ask these questions of their biomedical engineering teams.

Communicating risk to patients

Health professionals are responsible for talking to their patients about risks and benefits of using a medical device. This enables patients to provide informed consent. Patients and consumers of medical devices are encouraged to ask their health professional questions about their medical devices, and health professionals are referred to the guidance for patients and consumers, to see example questions that they may be asked.

Health professionals also need to be prepared to talk to their patients if a security vulnerability is discovered:

- Usually, the TGA or the medical device company will tell clinicians about vulnerabilities that require action from a health professional.
- Sometimes, the public may learn about a cyber security vulnerability in a medical device before clinicians, the TGA, or even the device manufacturer. If this happens patients may come to their health professional for help.

To prepare for questions about cybersecurity from patients, consider:

- proven therapeutic benefit provided by the medical device versus risk of the vulnerability being exploited
- potential consequences, especially clinical implications, if the vulnerability is exploited
- options to mitigate risks and associated timeframes
- risks associated with a medical device software or firmware update
- long-term solutions to eliminate or reduce risks

To help inform patients about medical device cyber security, the TGA has developed information for consumers.

Guidance for small business operators

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

The commencement of the Notifiable Data Breach scheme is an additional incentive for improved medical device cyber security. From February 2018, agencies and organisations regulated under the *Privacy Act 1988 (Cth)* (Privacy Act) with personal information security obligations are required to notify affected individuals and the Office of the Australian.

Information Commissioner (when a data breach is likely to result in serious harm to individuals whose personal information is involved in the breach. Notifiable data breaches may give rise to complaints and other regulatory action under the Privacy Act.

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

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

The Essential Eight

Mitigation strategies to prevent malware delivery and execution

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

Mitigation strategies to limit the extent of cyber security incidents

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

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

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

7. **Multi-factor authentication**—to protect against risky activities – Stronger user authentication makes it harder for adversaries to access sensitive information and systems. Multi-factor authentication should be implemented for all remote access users.

Mitigation strategies to recover data and system availability

8. **Daily backups**—to maintain the availability of critical data – This is important to ensure information can be accessed again following a cyber security incident. Backups should be tested in line with relevant medical information standards.

Guidance for large-scale service providers

The following medical device cyber security guidance[3] is predominantly applicable to administrators and engineers responsible for supporting healthcare services that are provided to the population, typically in medium to large health and medical service environments.

This guidance builds on the guidance provided for small business operators and highlights considerations that are applicable to large-scale healthcare providers, which might also be critical infrastructure. Many aspects are also applicable to small business operators. Guidance for cyber security of medical devices is important in this context as the continuous operation of health services can be disrupted by a successful cyber-attack, with cyber security vulnerabilities in a medical device being an accessible entry point for an attack.

Risk management strategy

Users responsible for implementing medical devices in critical health services should develop a clear and well documented risk management strategy. The primary goal is to develop an environment where risk to patients is minimised. The strategy will need to be revised as new types and classes of connected medical devices are added to the healthcare environment.

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

Consider:

- Reducing the attack surface of the biomedical environment. This involves isolating networks from any untrusted network such as the internet, disabling any unused ports and services, only allowing real-time connectivity to external networks with a defined business requirement and using unidirectional networks with an air gap where possible.
- Physical security of medical devices—restricting physical access to controls is appropriate in some operating environments. This must be closely managed to ensure usability of systems is not adversely affected.
- Expert cyber security services (either in-house or consultants) may be helpful to develop an understanding of how defendable the biomedical environment is. Examples include:
  - penetration testing to find vulnerabilities that could be exploited
  - cyber security operations centres/security information
  - event management services to monitor for threats

Outputs of these types of services may allow an organisation to complete higher quality risk assessment and develop more robust risk management strategies.

Good risk management strategies can also be developed by applying relevant standards, shown in the table below, and by reviewing and implementing risk management strategies from other industries.

Table 1: Standards that may be applied by service providers

Standard*	Scope
IEC 80001 (series)	Application of risk management for IT-networks incorporating medical devices
ISO/IEC 15408 (series)	Evaluation criteria for IT security
ISO/IEC 30111	Resolve potential vulnerability information in a product
ISO 27799	Health informatics—Information security management in health using ISO/IEC 27002

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

The USA's National Institute of Standards and Technology (NIST) cyber security framework is another globally accepted approach by the cyber security community as a way to address cyber security risks throughout the life cycle of an organisation's management of risk. The framework describes a series of concurrent and continuous cyber security functions that underpin a cyber security risk management strategy.

- **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

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

Cross-functional collaboration

Collaboration is essential for effective cyber security control of medical devices in healthcare organisations. Healthcare service providers should aim to facilitate an environment that drives cross-functional collaboration between the biomedical, clinical support and IT teams, helping all areas to develop a better understanding of the work completed within each team.

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

Collaborative procurement

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

- Incentivise procurement teams to work with IT and biomedical teams on the procurement of new medical devices to provide informed advice on appropriate security measures for the specific healthcare service provider. This will help ensure that cyber security is a measurable factor in procurement.
- Questions to ask during the procurement process may include:
  - What security measures have been built into the device?
    - What measures are in place to protect patient safety?
    - What measures are in place to protect the confidentiality, availability and integrity of patient data?
    - How has security been addressed at each level, e.g., hardware, firmware, OS, network, and user interface?
  - What security protocols and frameworks have been used?
  - What IT environmental requirements are needed for secure operation of the device?

  - What are the known cyber security vulnerabilities for the device?
  - Has the manufacturer assessed the cyber security of key components within the device (i.e. the supply chain)?
  - Does the 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 previously, and how where they managed?

Medical device inventory

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

- the device:
  - medical device name, operation and purpose
  - any secondary uses beyond intended purpose
  - location of device and any restrictions on physical access
  - device identifiers (serial numbers, MAC addresses, default/static IP addresses)
  - predecessor, successor and compatible devices
  - level of device criticality
- the software
  - device software versions (OS, applications and protocols)
- dependencies and interfaces
  - hardware, software and network dependencies
  - device interfaces (wired/wireless communications, external storage, input/output)
  - network ports for clinical and remote service use
- personnel
  - person(s) responsible for device security
  - primary users of the device (and their cyber security training level)
  - vendor and maintenance providers
- maintenance, support and end-of-life

- security and maintenance logging capabilities and configurations
- support agreements in place
- refresh cycles
- expected device life span
- end-of-life procedure / support for critical components (e.g. OS, legacy protocols)

Where possible, the organisation should request a software bill of materials from the manufacturer of the device to aid in inventory management.

Cyber security training

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

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

Apply defence-in-depth approaches

Defend against attacks using several independent methods. Such methods should include:

- general considerations, such as 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)

Isolate networks, applications, data sources, and systems

Networks, applications, data sources, medical devices, and systems should be isolated from each other, wherever possible, through applicable administrative; physical; firewall[4]; sandboxing, such as via jails or virtual machines (e.g., Qubes OS); access control; encryption; and other methods. For example, the biomedical network should be isolated from the corporate IT network. Isolation should also occur on a temporal basis where possible (that is, via limiting access to only those times when systems are in use). This will significantly reduce the risk of malware spreading.

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

Address legacy devices

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

Manage authentication

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

- Consider implementing multi-factor authentication for staff access to networks, especially in areas of high traffic and reduce privileges to only those required.
- Ongoing remote access to devices post sale by medical device manufacturers and sponsors should be an exception, not the rule. The exception is where remote access is considered necessary for the intended use of the device and where the benefits of this access outweigh the risks. Multi-factor authentication should be implemented with privileges reduced to only those required.
- Complete regular reviews of network access. These must be managed to ensure usability, safety, and security of systems is not adversely affected.
- Avoid the use of hard-coded passwords and default accounts.
- Avoid sharing credentials. Ideally each user has their own account and credentials.
- Ensure that systems and procedures are in place to remove access control from staff who leave the organisation.

[4] Administrators should consider the use of multiple firewalls (and of various types) at the network, server, client, application, and individual network-attached device levels/layers. The types of firewalls chosen might include packet-filtering, stateful inspection, circuit-level gateways, application-level/proxy gateways, or next-gen.

Secure remote access

- Remote access to healthcare service networks increases the window of opportunity for adversaries. Remote access should only be allowed when required.
- Consider restricted access when using applications remotely and time-limited access.
- Multi-factor authentication and encryption is critical for remote access.

Restrict administrative privileges

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

Monitor and respond

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

- Healthcare service providers should ensure they have visibility over their networks.

Monitoring should occur in the following places:

  - Monitor IP traffic on biomedical network boundaries for abnormal or suspicious traffic
  - Monitor IP traffic within the biomedical network for malicious connections
  - Use host, network, and wireless intrusion detection systems to detect malicious software and attacks
  - Consider the use of intrusion prevention systems for automated response to detected intrusions
  - Use login analysis to detect stolen credentials usage or improper access, verifying all anomalies with quick phone calls
  - Watch account / user administration actions to detect access control manipulation such as elevating a user's privileges that would not normally require it

Monitoring the broader environment for potential threats—this includes monitoring and responding to threat intelligence sources, such as CERT alerts and any alerts issued by the TGA, sponsor or manufacturer. Depending on the technical capacity of the team, this might include developing a register of known vulnerabilities.

- Service providers can apply threat information to manage risks according to standards and guidelines. The information can be applied to procurement process, hardening the

security of the medical devices and their environment, or simple security audits in the form of regular penetration tests.

Cyber security and operational planning

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

- Ensure cyber security is proactively assessed as a key element in risk assessments and business continuity planning; proactively implementing appropriate cyber controls is essential to risk management.
- Develop a cyber security strategic plan, which includes a cyber specific risk assessment and response strategies. The plan should have clearly defined event response procedures that define the responsibilities of each department (in the hospital or other service provider) in the event of an incident, and emphasise the importance of each area being familiar with these procedures.
- Network threat modelling using approaches such as the MITRE ATT&CK framework are also recommended to improve the cyber resilience of devices and the organisation more broadly.

Reactive actions

Following a known or suspected cyber security breach via a medical device or on the biomedical network, service providers should be able to consult their cyber security strategic plan to understand the steps that need to be taken in the given situation. Some actions to consider include the following[5]:

- **Report the security breach to the device manufacturer or sponsor, and to the TGA as an adverse event if appropriate. The Australian Cyber Security Centre may also be a useful source of information to help overcome the breach.**
- Work with clinicians to understand the implications of disabling network connectivity as a risk mitigation strategy on a case-by-case basis. If clinically acceptable, disconnect the medical device from the network.
- Work with clinicians to communicate any risks to patients, on a case-by-case basis. These risks may include the potential consequences of the breach, options to mitigate the risk, long term solutions to address cyber security breach and vulnerabilities, and discussion on the benefits of the device versus the cyber security risk.
- Work with cyber security team and the device manufacturer to manage the vulnerability and to restore the system.
- If any patient data was involved, inform risk management so that the potential breach can be handled in accordance with applicable obligations under the Privacy Act, including in accordance with the Notifiable Data Breach scheme and any related OAIC requirements.
- Avoid installing un-validated patches or making any changes to the device configuration without explicit instructions from the manufacturer.

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

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

Measuring cyber security resilience

When considered collectively, the guidance provided for healthcare service providers can form the basis for assessing organisational maturity concerning medical device cyber security. This may be achieved by developing a matrix system, which can be used to understand areas of strength and areas where additional effort is required (e.g. Table 2). Healthcare service providers should develop low, medium and high criteria suitable to their organisation. These criteria should be tested as follows:

- Conduct cyber security exercises at least annually to test the whole-of-organisation's response and recovery plans.
- Assess maturity annually to ensure continued attention to providing a cyber secure environment for the use of medical devices.

Alternatively, if appropriate to an organisation's cyber security risk and resources, the NIST framework can be applied as a robust cyber security maturity assessment.

Table 2: Example cyber security self-assessment matrix

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

Cyber security considerations are not exhaustive; 'Low', 'Medium' and 'High' refer to how well the protocols and practices related to the cyber security considerations are established and implemented.

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

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

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

Medical device users

Users of medical devices are encouraged to monitor cyber security threats and participate in cyber security intelligence and threat sharing as appropriate, using the above modes.

For example, the Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience includes a Health Sector Group, which may be relevant for large scale service providers. TISN facilitates information sharing between members of the group on issues relating to critical infrastructure in the health sector, appropriate measures and strategies to mitigate risk and improve organisational resilience. TISN have published a number of documents that are relevant to cyber security threat sharing.

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).

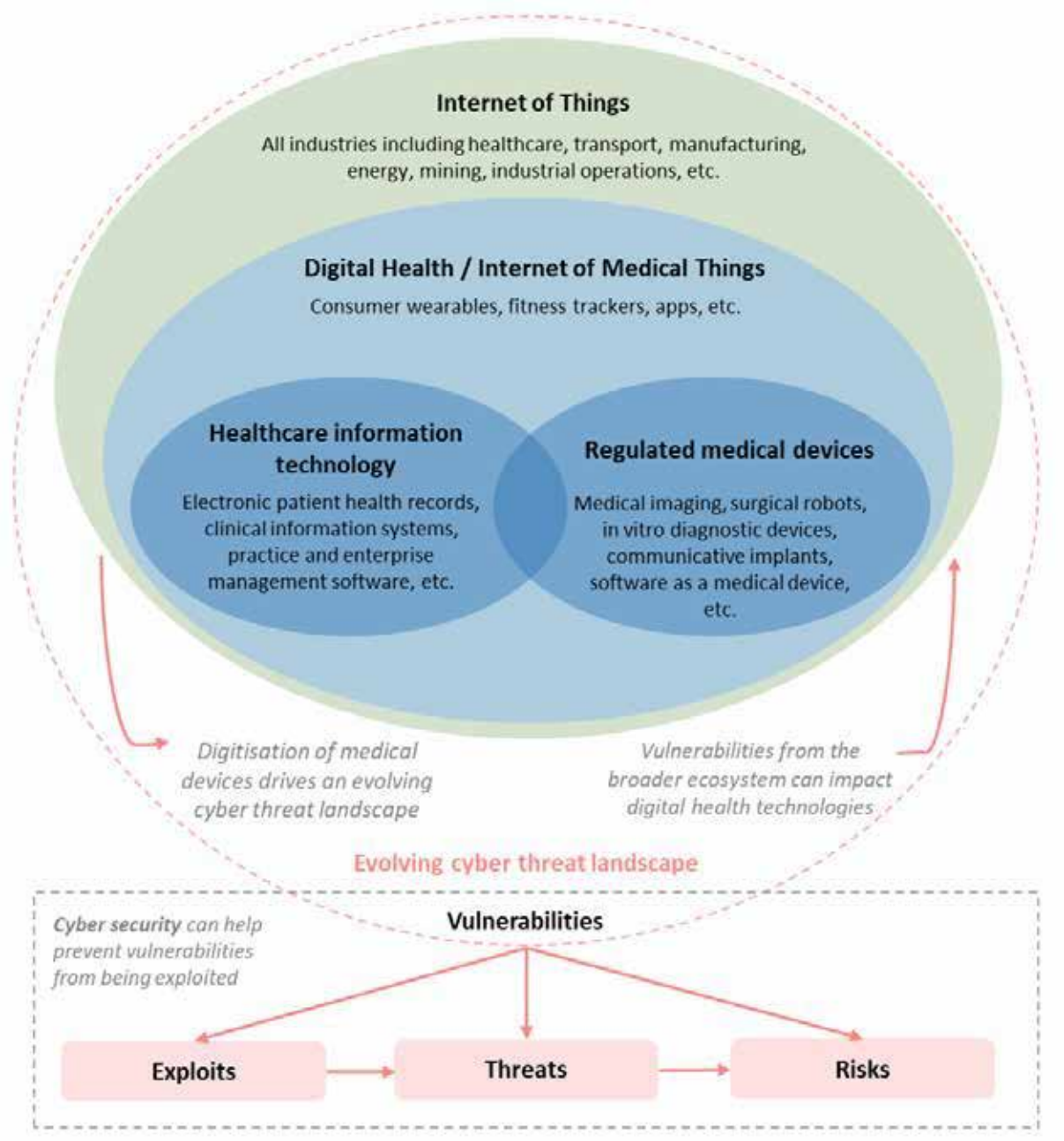
Health technology and cyber security

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 1: 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 and 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 3: 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

Trend name	Trend observations	Cyber security considerations
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
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 • 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 • 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

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	Minor updates	Medical Device Surveillance Branch	March 2021
V1.2	Changes to further align with the Australian Cyber Security Centre	Medical Device 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

Reference/Publication #