Complying with cybersecurity requirements for medical devices

WHITE PAPER

sgs.com

SGS

Cybersecurity is a critical aspect of medical device regulation as the healthcare sector seeks to adopt new technologies to improve patient care, while simultaneously protecting patient data and safety.

Compliance with the Therapeutic Goods Administration (TGA) requirements is essential for ensuring the safety and integrity of medical devices in Australia.

Understanding and adhering to TGA guidelines for cybersecurity means manufacturers can mitigate cybersecurity risks, while safely contributing to the advancement of healthcare technology in the digital age.

In this white paper, we shed light on the importance of cybersecurity in medical devices, including topics around regulatory compliance, current issues, challenges, and opportunities for improving cybersecurity measures in medical devices for manufacturers and sponsors.

Cybersecurity – a regulatory obligation

Medical devices cannot generally be supplied in Australia unless they are included on the Australian Register of Therapeutic Goods (ARTG) (2).

Inclusion on the ARTG requires considerations that span the life of a medical device, including:

- pre-market via conformity assessment
- market authorization 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.

Complying with TGA requirements for cybersecurity is not only a regulatory obligation but also essential for ensuring the safety and effectiveness of medical devices (1).

By implementing robust cybersecurity measures, manufacturers can minimize the risk of cyber threats and protect patient safety and data privacy.

Moreover, adherence to TGA requirements can enhance manufacturers' credibility and reputation in the healthcare industry, fostering trust and confidence among healthcare professionals and patients.

Industry relevance

Cybersecurity is crucial for internet-connected medical devices and hospital networks, aiming for high efficiency and advanced services. Yet, this connectivity elevates cybersecurity risks.

> The US Cyber Threat Intelligence Integration Center further highlights the **growing danger** for medical technology, noting that worldwide randsomware attacks targeting the healthcare sector have **nearly doubled** since 2022. As the frequency of cyberattacks escalates, medical records are increasingly targeted, and vital equipment is either disrupted or manipulated, putting patients' lives at serious risk (5).

A significant recent cyber-attack in Australia concerning medical devices was the data breach affecting MediSecure, a prescription delivery service. In this incident a hacker stole personal and health information related to prescriptions from approximately 12.9 million Australians, marking one of the largest data breaches in the country. This incident exposed vulnerabilities in the health system's connected medical data handling processes.

Globally, regulators now require resilience against these threats for medical devices, prompting stricter regulations and mandatory cybersecurity assessments.

Active medical devices such as pacemakers, drug delivery pumps, lung ventilators and dialysis machines are increasingly connected to the internet, healthcare organizations' networks, and other devices, to enhance their functionality and the ability of healthcare providers to treat patients.

Increasingly, active medical devices can be controlled via a mobile phone and data can be transmitted remotely to the treating physician. More recently, rapid advances in computing technology and software production have led to an explosion of medical apps or software as medical devices (SaMD) (3).

The connectivity of medical devices to the internet and networks facilitates information sharing and treatment delivery, but it also exposes medical devices to the risk of potential cybersecurity threats.

Although threats and vulnerabilities cannot be eliminated, they can be reduced and managed by implementing good cybersecurity practices (3).

The threats of failing to address cybersecurity

Healthcare systems are prime targets for cyber-attacks due to the valuable patient data medical devices hold, including personal information, medical records, and financial details. The increasing connectivity of medical devices, electronic health records (EHRs), and telemedicine platforms creates additional entry points for hackers.

Cyber-attacks can disrupt healthcare services, by compromising patient safety, causing financial losses and damaging healthcare providers' reputations.

> In Australia, the Government has been advised by MediSecure that approximately **12.9 million individuals** may have had their personal and health information relating to prescriptions, and healthcare provider information exposed by a cybersecurity incident (6).

Challenges of cyber attacks in healthcare

- **Patient privacy breaches:** Unauthorized access to patient records can lead to identity theft, insurance fraud, and other malicious activities.
- **Compromised medical devices:** Hackers can exploit vulnerabilities in medical devices, potentially causing harm to patients or interfering with critical medical procedures, a situation that should never be allowed to happen.
- **Financial implications:** Cyber-attacks can result in significant financial losses due to remediation costs, legal fees, regulatory fines, and reputational damage, putting a heavy strain on the healthcare system's resources (4).

Wider implications of cyber breaches

Following the MediSecure cyber breach, MediSecure confirmed that approximately 12.9 million Australians who used the MediSecure prescription delivery service during the approximate period of March 2019 to November 2023 were impacted by this incident based on individuals' healthcare identifiers. However, MediSecure is unable to identify the specific affected individuals despite making all reasonable efforts due to the complexity of the data set (7). Threats can emerge with vulnerabilities and adversarial motives to exploit these vulnerabilities, a situation can potentially to cause harm.

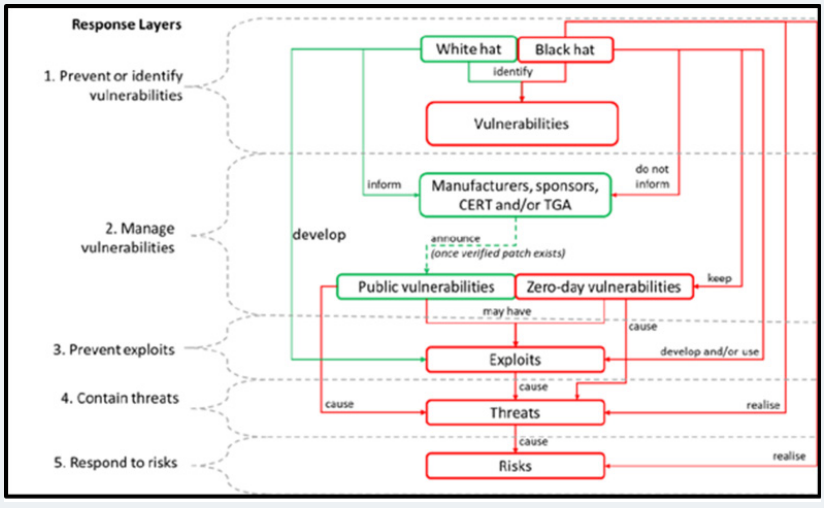
A growing threat

This breach highlights the increasing vulnerability of Australian healthcare systems to cyberattacks, particularly as more medical devices become connected to the internet.

Vulnerabilities

The incident emphasizes the importance of robust cybersecurity measures within healthcare providers and related services to protect patient data. The threat on patient privacy, such that data may be exposed to unauthorized 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 objectives. This is best described in Figure 1 as below (2):

FIGURE 1: VULNERABILITIES, EXPLOITS, THREATS, RISKS AND ADVERSARIES



OAIC cyber incident findings

FIGURE 1

According to OAIC (8) (Office of the Australian Information Commissioner), from July to December 2023, **527 NOTIFICATIONS** were received (up 9% compared to July to December 2023:

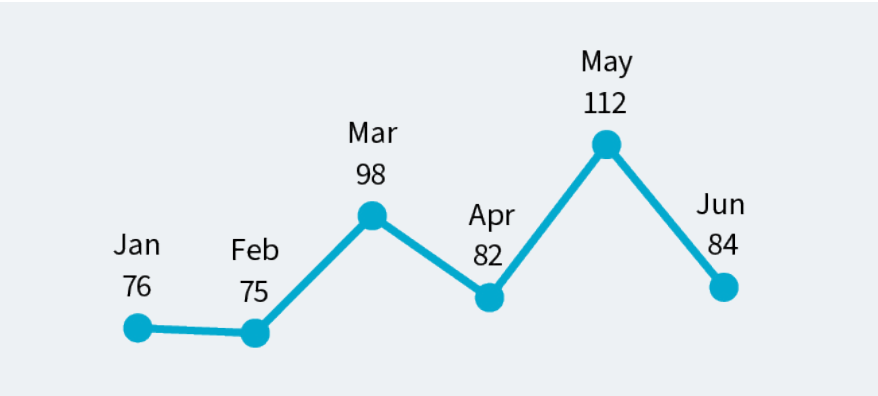


FIGURE 2

TOP 5 SECTORS TO NOTIFY DATA BREACHES

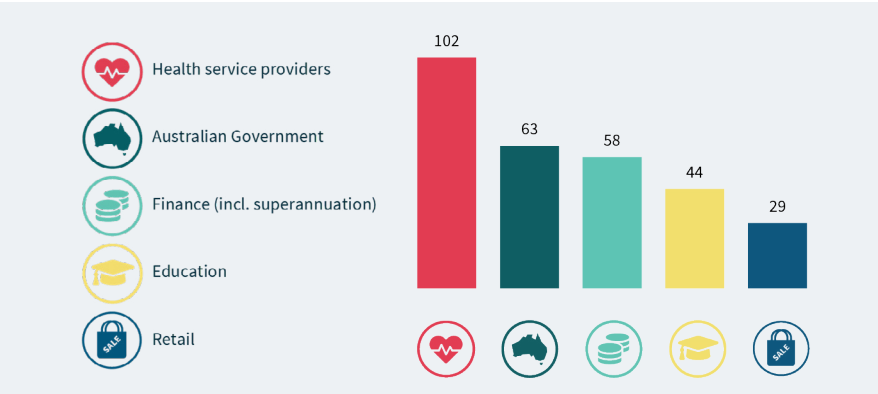


FIGURE 3

SOURCES OF DATA BREACHES

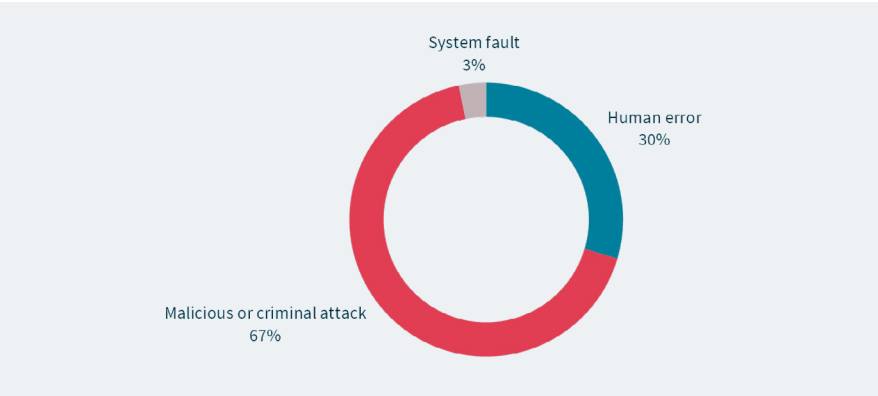
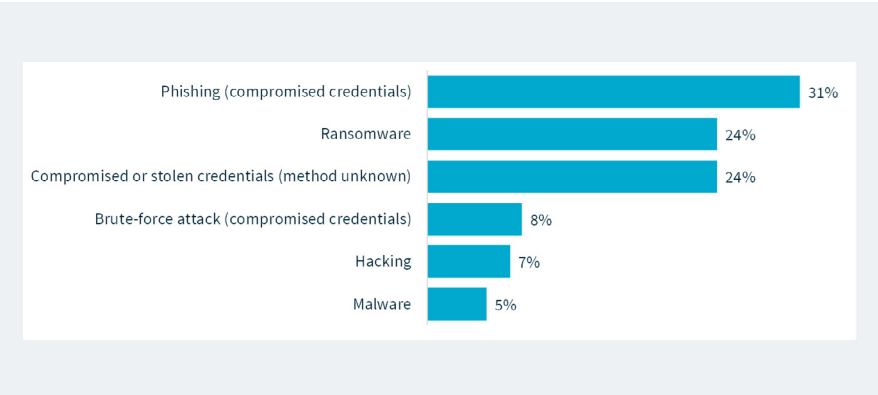
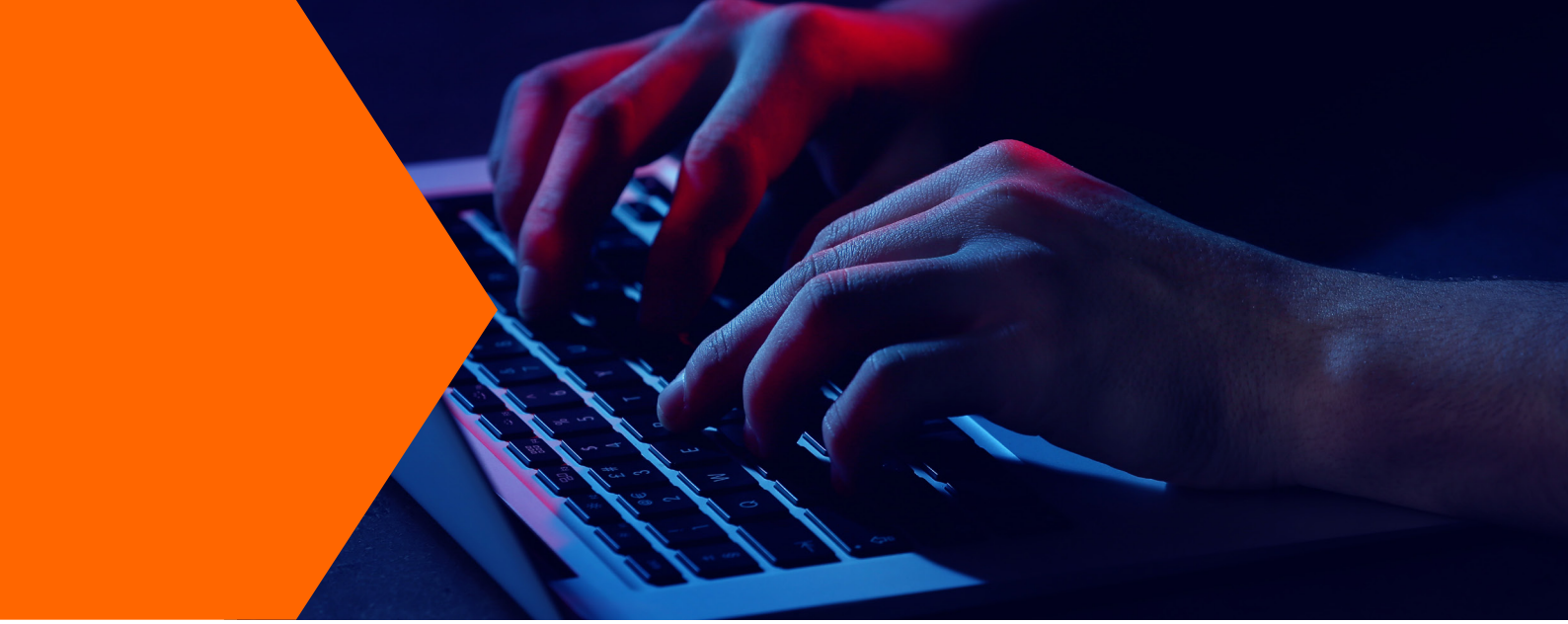


FIGURE 4

CYBER INCIDENT BREAKDOWN





How can healthcare providers improve cybersecurity?

The following measures are recommended in order to defend the healthcare system from cyber threats:

- **Robust risk assessment and management**: Healthcare providers should conduct regular assessments of system vulnerabilities and identify potential risks. Organizations should develop and implement comprehensive risk management plans tailored to the specific needs of healthcare organizations. To mitigate human error risks, a culture of cybersecurity awareness should be fostered, and training should be provided to all staff members.
- **Implementing strong technical controls**: Healthcare providers should deploy advanced technologies, such as encryption, anti-phishing and data loss prevention, to protect networks and sensitive data. Ensure regular patching and updating of software and systems to address known vulnerabilities. Implement and employ multi-factor authentication and strong access controls to safeguard patient records and limit unauthorized access.
- **Continuous monitoring and incident response:** Establish robust monitoring systems to detect and respond to cyber threats promptly. Develop an incident response plan to minimize a cyber-attack's impact and facilitate swift recovery.

Further defense against cyber threats

Entities must take appropriate and proactive steps to protect against a range of cyber threats.

The OAIC encourages organizations to:

- Implement multi-factor authentication for access to business systems, online services and data repositories, and for users when they perform a privileged action (using phishing-resistant multi-factor authentication will provide entities additional security that is not as susceptible to sophisticated cyber-attacks).
- Where multi-factor authentication is unavailable, enforce password management policies such as password complexity requirements or the use of strong passphrases - external site, and ensure passwords are not being reused across systems.
- Layer security controls to avoid a single point of failure.
- Ensure users have appropriate levels of access to information assets depending on their role and responsibilities; monitor and regularly review accounts with more access permissions, removing access privileges where no longer required.
- Implement robust security monitoring processes and procedures to detect, respond to and report incidents, or unusual or suspicious activity promptly.

In Australia, cybersecurity incidents were the cause of **38% of all data breaches** from January to June 2024 (8).

Working with TGA regulations

Manufacturers and sponsors must demonstrate how they will gather information regarding emerging cybersecurity vulnerabilities that may impact the safe operation of their medical device, and demonstrate assessment and any relevant action as part of ongoing risk management (2).

This is necessary to ensure that a medical device included in the ARTG continues to meet the requirements of the TGA's Essential Principles, outlined below.

This can be achieved by ensuring that complaint monitoring processes for manufacturers and sponsors include cybersecurity 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 cybersecurity vulnerabilities and threats that they discover.

In Australia, medical devices and in vitro medical devices are regulated under Therapeutic Goods (Medical Devices) Regulations 2002, Therapeutic Goods Act 1989 & TGA Essential Principles, respectively.

These require (2):

- 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.
- 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 minimize any risks associated with the use of the device.
- Essential Principle 12.1(5): 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.

In 2023, the Identity Theft Resource Center reported **2,365 cyberattacks** across all connected technologies, affecting 343,338,964 victims. This marks a **72% increase in data breaches** compared to 2021, which was itself a record (5).

Cybersecurity compliance standards to help

In Australia, the primary compliance requirement for cybersecurity in medical devices is governed by the TGA through the Therapeutic Goods Act 1989, which mandates that medical devices must meet specific cybersecurity standards, essentially requiring manufacturers to design and implement robust security measures to protect patient data and device functionality from cyber threats. This often aligns with international standards like ISO/IEC 27001, ISA/IEC 62443 and ISO 14971, which focus on risk management and security controls within medical devices.

- Complementary: These standards can be used together to create a comprehensive cybersecurity program for organizations.
- Organizations can leverage the principles and controls outlined in ISO/IEC 27001 to implement a robust ISMS that also addresses the security requirements of their IACS, as defined by ISA/IEC 62443.
- Both ISO 14971 and ISO/IEC 27001 focus on the risk management framework and require the organization's risk assessment plan, risk report, and risk treatment plans to protect the confidentiality, integrity and availability of the assets.

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

Key aspects of medical device cybersecurity compliance (it can be addressed through ISO/IEC 27001)

Risk Management	Performing thorough risk assessments to identify potential cybersecurity vulnerabilities in the device design, and throughout its lifecycle.
Secure Development Practices	Implementing secure coding practices, input, validation, and encryption mechanisms to protect sensitive data within the device.
Access Control	Managing user access levels to the device and its functions to prevent unauthorized modifications or data access.
Network Security	Implementing appropriate network segmentation and security protocols to safeguard the device from external threats.
Patch Management	Maintaining up-to-date software patches and firmware updates to address known vulnerabilities.
Incident Response Plan	Having a defined process to detect, respond to, and contain cyber incidents that may affect the medical device.
Data Privacy	Complying with data privacy regulations like the Australian Privacy Principles (APP) when handling patient data collected by the medical device.

Evolving challenges

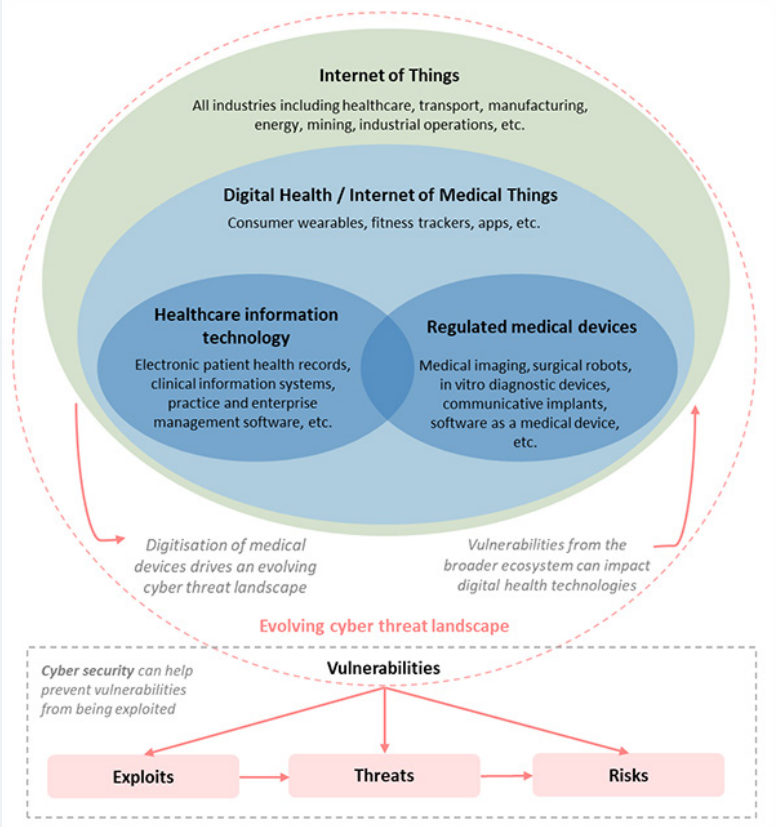
The digitalization of consumer and professional health technology is rapidly gathering traction, with increased application of wireless communication, cloud services, artificial intelligence (AI) and other technologies.

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 cybersecurity implications from an evolving cyber threat landscape.

Increased connectivity and digitization of health technologies drive 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



Conclusion

One of the key requirements set forth by the TGA is the need for medical device manufacturers to conduct comprehensive risk assessments to identify potential cybersecurity vulnerabilities.

This involves evaluating potential threats to the device's security, assessing the likelihood of these threats occurring, and determining the potential impact on patient safety and data integrity. Manufacturers must then implement appropriate risk mitigation measures to address identified vulnerabilities and minimize risks to an acceptable level. Additionally, the TGA emphasizes the importance of incorporating cybersecurity principles into the design and development of medical devices. This includes implementing secure design practices, such as encryption, authentication, and access controls, to prevent unauthorized access to the device and protect sensitive data. Manufacturers are also encouraged to regularly update and patch their devices to address newly discovered vulnerabilities and ensure ongoing security (1).

In conclusion, cybersecurity is a critical aspect of medical device regulation, and compliance with TGA requirements is essential for ensuring the safety and integrity of medical devices in Australia (1). By understanding and adhering to TGA guidelines for cybersecurity, healthcare providers and medical device manufacturers can advance technological innovation while mitigating risks and protecting patient safety, data privacy, and the integrity of the healthcare system.

Recommendations for manufacturers

In summary, the TGA has established clear guidelines for medical device manufacturers to address cybersecurity concerns. These requirements are outlined in various regulatory documents, including the Australian Regulatory Guidelines for Medical Devices (ARGMD), and specific guidance documents on cybersecurity. Furthermore, the TGA requires medical device manufacturers to provide documentation demonstrating compliance with cybersecurity requirements. This includes detailed information on the device's cybersecurity features and capabilities, and evidence of risk assessments and risk mitigation measures undertaken during the device's development and lifecycle.

Important points to remember:

- **Collaboration with healthcare providers:** Manufacturers should engage with healthcare providers to understand their cybersecurity needs and concerns regarding medical devices.
- **Continuous monitoring and improvement:** Cybersecurity practices must be regularly reviewed and updated to address emerging threats and technological advancements.
- **Transparency and communication:** Manufacturers should be transparent about the cybersecurity capabilities of their medical devices and communicate effectively with users.

Why SGS?

SGS is the world's leading Testing, Inspection and Certification company. We operate a network of over 2,500 laboratories and business facilities across 115 countries, supported by a team of 99,500 dedicated professionals.

Combining decades of digital expertise worldwide and the latest knowledge of cybersecurity trends and technologies, SGS can help you meet the highest data defense and system integrity measures.

For more information, visit our Digital Trust Assurance web page or contact us today.

References and Appendix

References

1. Understanding TGA Requirements for Cybersecurity in Medical Devices, MedSec Testing - https://medsectesting.com/tga-cybersecurity-and-testing-requirements-for-medical-devices
2. Complying with medical device cyber security requirements, TGA - https://www.tga.gov.au/resources/guidance/complying-medical-device-cyber-security-requirements
3. Cybersecurity for medical devices, Medical Technology Association of Australia - https://www.mtaa.org.au/cybersecurity-medical-devices
4. Defending the Australian Healthcare System from Cyber Threats, Deloitte - https://www.deloitte.com/au/en/Industries/health-human-services/blogs/defending-the-australian-healthcare-system-from-cyber-threats.html
5. Navigating Cybersecurity Challenges in MedTech, SGS - https://www.sgs.com/en-au/news/2025/01/cc-q4-2024-navigating-cybersecurity-challenges-in-medtech#reference
6. MediSecure cyber security incident, Department of Home Affairs - https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-coordinator/medisecure-cyber-security-incident
7. MediSecure statement on cyber security incident, MediSecure - https://medisecurenotification.wordpress.com/
8. Notifiable Data Breaches Report: January to June 2024, OAIC - https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2024
9. Healthcare Cybersecurity, Data Breach & Cybercrime Statistics in Australia - https://eftsure.com/en-au/statistics/healthcare-cybersecurity-data-breach-cybercrime-statistics-in-australia/

Appendix

Additional relevant information can be found at:

- https://www.tga.gov.au/resources/legislation/therapeutic-goods-medical-devices-regulations-2002
- https://www.tga.gov.au/resources/legislation/therapeutic-goods-act-1989
- https://www.tga.gov.au/resources/guidance/complying-medical-device-cyber-security-requirements
- https://www.tga.gov.au/resources/resource/reference-material/medical-device-cyber-security-information-users
- https://www.cyber.gov.au/
- https://www.tga.gov.au/node/287250
- https://www.tga.gov.au/resources/resource/checklists/essential-principles-checklist
- https://www.tga.gov.au/resources/acronyms-and-glossary-terms#id_9257
- https://www.nema.org/standards/view/manufacturer-disclosure-statement-for-medical-device-security?key=67ri900e6rt5af#download
- https://www.cyber.gov.au/about-us/about-asd-acsc/who-we-are
- https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight
- https://www.tga.gov.au/resources/resource/reference-material/uniform-recall-procedure-therapeutic-goods-urptg
- https://www.tga.gov.au/how-we-regulate/compliance-and-enforcement-hub/compliance-management
- https://www.oaic.gov.au/privacy/notifiable-data-breaches
- https://www.imdrf.org/

When you need to be sure

SGS Headquarters
1 Place des Alpes
P.O. Box 2152
1211 Geneva
Switzerland

sgs.com