Information security for the medical device industry

CREATE A SOLID FOUNDATION FOR CYBERSECURITY & DATA PRIVACY

SGS

Table of contents

Overview 3

The growing need for cybersecurity 4
- Unprecedented levels of data sharing....4

IoMT in healthcare 5
- Medical devices: A target for healthcare data breaches....5
- Supply chain links are increasingly brittle....7
- Safety & security risks for medical devices....9

Case studies 10

Cybersecurity preparedeness regulations 12
- FDA & cybersecurity of medical devices....12
- Global data privacy & medical device cybersecurity regulations..13

ISO/IEC 27001: An ISMS governance framework 14
- A holistic approach to managing information security risk....14
- ISO/IEC 27001 structure....16
- Pinpoint vulnerabilities in your organization & supply chain....16

Business & financial benefits of certification 17

How to get certified 19

SGS: A trusted partner 22
- Transitioning from ISO/IEC 27001:2013 to ISO/IEC 27001:2022.. 22
- Why SGS?.... 23

Next steps: Transition or first-time certification 24

References 25

Overview

With a focus on the medical device industry, this paper provides software developers, hardware developers, and manufacturers with an understanding of the necessity and benefits of cybersecurity preparedness that can be achieved through the implementation of an Information Security Management System (ISMS). The implementation of an ISMS is a foundation for industry certification, which is also a beneficial next step for organizations seeking to strengthen their security posture and marketability. Although an ISMS covers many areas of technology, here we delve into the cybersecurity component of it – an emergent top priority for both business and technology leaders in the healthcare industry.

You will gain an understanding of:

- Why cybersecurity and data privacy have become key foci of information security management.
- Why cybersecurity and data privacy are a growing concern for the medical device industry.
- How interconnectivity of supply chains increases risk.
- How medical device recalls and healthcare data breaches have impacted organizations.
- How ISO/IEC 27001 certification constructs a framework for enhancing your resilience in the face of cybersecurity threats and data breaches.
- How to obtain an independent ISO/IEC 27001 certification.

SGS' EXPERIENCE IN DELIVERING ASSESSMENTS AND PROVIDING CERTIFICATIONS FOR ORGANIZATIONS ACROSS THE HEALTHCARE SUPPLY CHAIN INFORMS THE CONTENT OF THIS PAPER. OTHER INDUSTRY SOURCES HAVE ALSO BEEN REFERENCED.

The growing need for cybersecurity

UNPRECEDENTED LEVELS OF DATA SHARING

While information security has always been tasked with protecting organizational data, the scope of this responsibility was traditionally limited to information contained in paper records and data travelling within an organization's 'four walls' or on its private network. What happens when data is transmitted through the Internet and is stored in a shared cloud network? This question prompts the emergence of cybersecurity – an area of information security that has become top of mind for both business and technology leadership across industry. Cybersecurity focuses entirely on computer and web-related security, while information security covers all forms of securing information. As such, cybersecurity is a subset of information security, with an overlap occurring since both exist to protect the confidentiality, integrity, and availability of data.

The amount of data being stored, processed, and transmitted over the Internet today is unprecedented. This is accelerated by 5G networks and advancements in wireless communications that are enabling the connectivity of billions of devices with the ability to share data, also at unprecedented levels. This digital interconnectivity presents cyber criminals with more avenues to compromise and more data to gain. The wider an organization's cyber footprint, the larger its attack surface. Although cybersecurity dates back to the advent of the Internet, its importance and necessity has never held more importance than it does today.

CYBERSECURITY IS THE PROTECTION OF COMPUTER SYSTEMS AND NETWORKS FROM INFORMATION DISCLOSURE, THEFT, OR DAMAGE TO ELECTRONIC DATA, AS WELL AS FROM THE DISRUPTION OR MISDIRECTION OF THE SERVICES THEY PROVIDE.

The need for cybersecurity is fuelled by the Internet of Things (IoT). The IoT is a network of dedicated physical objects (things) that contain embedded technology allowing for 'cloud-based' communication or wireless communication with other technology, business, financial, or legal systems. This enables the capture of data and events in real-time, from which a company can learn behavior and usage, react with preventive action, or improve business processes. The IoT is a foundational capability for the creation of a digital organization.[1] In the healthcare industry, data stored in and transmitted through digital medical devices exposes service providers to a range of cybersecurity threats.

IoMT in healthcare

MEDICAL DEVICES: A TARGET FOR HEALTHCARE DATA BREACHES

Digital transformation in healthcare has augmented the production and use of medical devices that are IoT or IoMT (Internet of Medical Things) enabled. Although these devices have enhanced efficiency and have become critical in facilitating patient care, their increased deployment and use have widened the cyber landscape - presenting new opportunities for cyber criminals to seek data exposures. Medical devices are an easy entry point since security has not historically been critical in their design.[2]

IOMT DEVICES TRANSMIT AND CAPTURE DATA THROUGH THE FOLLOWING TECHNOLOGIES:

Examples of devices with these technologies include:

IMPLANTABLE DEVICES

- Pacemakers
- Insulin pumps

DIAGNOSTIC EQUIPMENT

- MRI machines
- Blood glucose monitors
- DICOM and PACS software

THERAPEUTIC DEVICES

- Ventilators
- Infusion pumps

WEARABLE DEVICES

- Smart watches

In the medical industry, the IoMT is also being used for:

- Remote patient monitoring (RPM) for people with chronic diseases and long-term conditions.
- Tracking patient medication orders.
- Tracking the location of patients admitted to hospitals.
- Connecting ambulances en route to medical facilities to healthcare professionals...

… and more.

Patient data or Protected Health Information (PHI) is being collected and transmitted via IoMT networks, with limited or no direction from patients or healthcare practitioners.

The healthcare industry is among the top three North American industries targeted by cyber criminals.

Why? Nearly everybody requires healthcare services, leading to the reality that nearly everyone's health information (PHI) is shared with service providers at some point in time. Due to the sensitive and personal nature of PHI, healthcare is a lucrative target for cyber criminals seeking financial ransom in exchange for stolen data. This data can also be used for identity theft and fraud. Attackers have used stolen credentials to obtain medical services or drugs. healthcare service providers have faced serious compliance penalties, fines, and reputational damages from such data breaches.

Generally, the healthcare industry has also invested less than other sectors in technologies needed to mitigate data breaches. A weak IT posture with respect to cybersecurity governance makes healthcare facilities more susceptible to cyberattacks. Poor incident response and remediation add to this susceptibility. Without the support of 24/7 data backups and a team of incident response experts, healthcare institutions have been more likely to pay financial ransom demands to avoid massive operational disruption.[3]

Unique to the healthcare industry, however, data breaches go far beyond posing risks to patient privacy and security. They also present a significant and critical risk to patient diagnosis and treatment; in other words, the safety of the patient. As a result, healthcare leadership and Boards have taken a keen interest in doing more to manage cyber risk.

Hospitals and end users are becoming more interested in knowing whether manufacturers or third parties are certified or compliant to product regulations and other legal requirements - and there is a push to choose third parties accordingly.

High-profile healthcare data breachest growing in frequency and scale

Ransomware demands into the millions of dollars and reputational damage for service providers.

Heightened scrutiny on information risk oversight responsibilities

"Boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril."

Luis A. Aguilar - US SEC Commissioner [4]

Cybersecurity dominates the IT agenda across industry

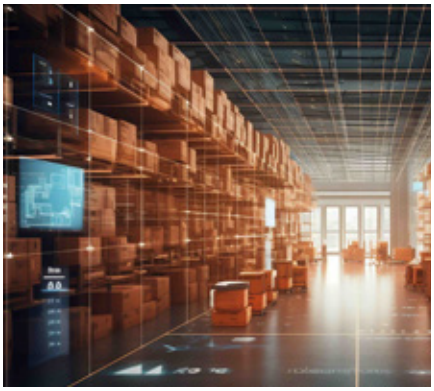
Gartner's Annual CIO Survey revealed that 66% of respondents planned to increase investment in cybersecurity in 2023.[5]

SUPPLY CHAIN LINKS ARE INCREASINGLY BRITTLE

In most cases, a healthcare service provider depends on numerous third parties including suppliers, developers, manufacturers, and distributors. Each player in the supply chain presents an opportunity for data exposure, through which data privacy can be compromised. An information security management system that incorporates a governance framework allows an organization to identify vulnerabilities and implement compensating or rectifying controls.

In the past, legal manufacturers of medical devices have not always considered security as a key consideration during the design and development phase. This is why older devices, still in use across healthcare today, may be in need of security features that could prevent data breaches. The common concept of state-of-the-art (SOTA) for medical devices implies that cutting edge technology is not essential so long as an established technology is serving its purpose within the device. This has resulted in legacy systems that require replacement, isolation, or patching as well as lack of standardization across devices.[6]

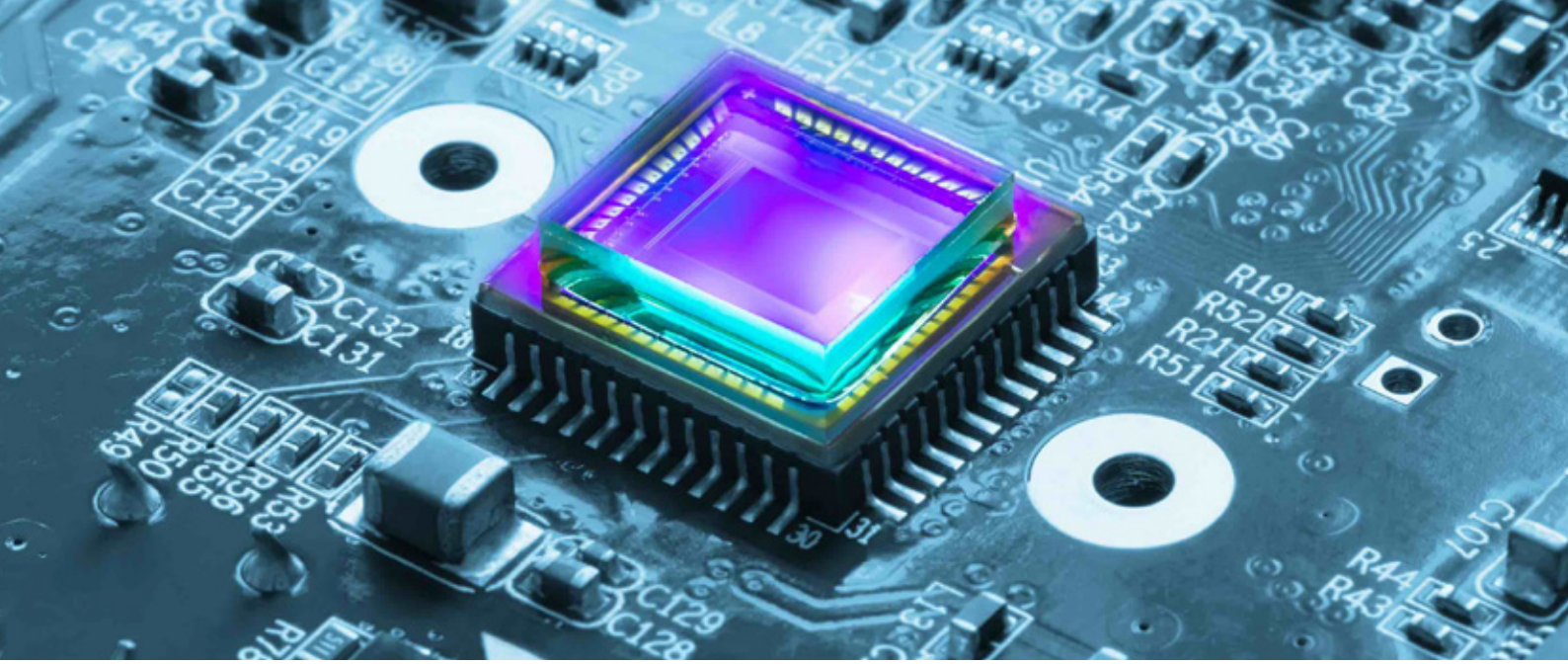
These systems were designed when cyber threats were less sophisticated so they inherently lack security features required to defend against new and emergent cyber attacks.



Risk assessment

Risk assessment is critical for organizations to determine whether older devices can be upgraded or whether they need to be replaced. Risk management is also critical for developers and manufacturers to identify and mitigate potential exposure of data in the future. Managing this risk must cover the whole lifecycle of a product, including risks posed during intended use and foreseeable misuse. Cybersecurity must be looked at as a whole - because third parties themselves may have security deficiencies that pave a way of entry for cyber criminals. If a risk, including cybersecurity risk, is known, the manufacturer cannot claim that it was unforeseeable, therefore it is now their responsibility.

Significant investments in security tools and employees have been made and healthcare technology leaders are now required to regularly report on the status of their cybersecurity programs, including the cybersecurity preparedness of their employees and vendors across the supply chain.



Legal manufacturers often leverage both software and firmware systems for their products to function effectively. These complex systems can contain source code from external parties (Software Of Unknown Provenance) that can be breached and manipulated, since their development origins are external and unknown. While a medical device legal manufacturer has gone through the steps to ensure cybersecurity preparedness, this same manufacturer needs to also look at the preparedness of their supplier who is developing their sensor software.

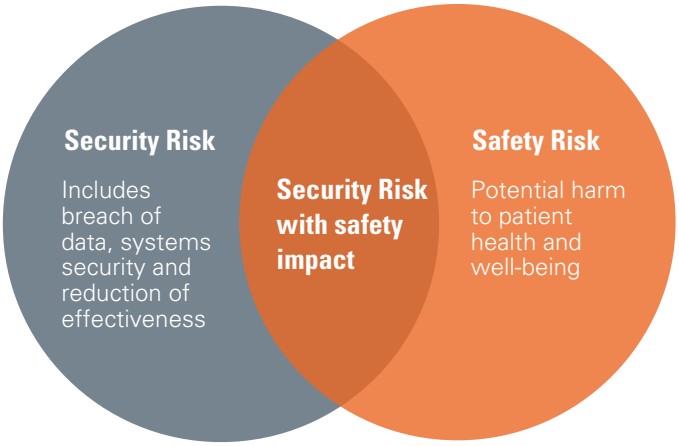
Developers needs to think all the way through to the end of life of a device incorporating its sensor. While cyber criminals can attempt to penetrate firewalls, they can also install malicious code into software, causing an effect to the end user or patient. The end user can be either the healthcare professional responsible for treating a patient or it can be the patient him or herself.

Examples of whole lifecycle risk related questions include:

In the case of a device storing PHI, what happens to the device when it is discarded at the end of its life? If a security patch needs to be installed on a device after a year's time, can this be carried out by the developer or can this be taken care of by the end user? What are the security implications if being carried out by the end user? What are the security implications if the end-user does not update the device?

Today's suppliers must undergo a cyber risk assessment that can validate them for 'Secure Design and Manufacture'. To reduce risks of using open-source software, each component must be assessed. A security analysis helps to understand the risk of use and highlight vulnerabilities. In addition, an important contract term for insurers is "supplier obligation management." Insurers must take appropriate steps to manage their supply chains by requiring that each supplier describe, and guarantee, the cyber health of their organization. In other words, suppliers must demonstrate their level of cybersecurity preparedness as a condition of becoming a supplier. This is becoming more and more of a common practice for organizations in the manufacturing and development spaces. All players across an organization's supply chain should create a solid framework for protecting sensitive data from a cyber breach.

SAFETY & SECURITY RISKS FOR MEDICAL DEVICES

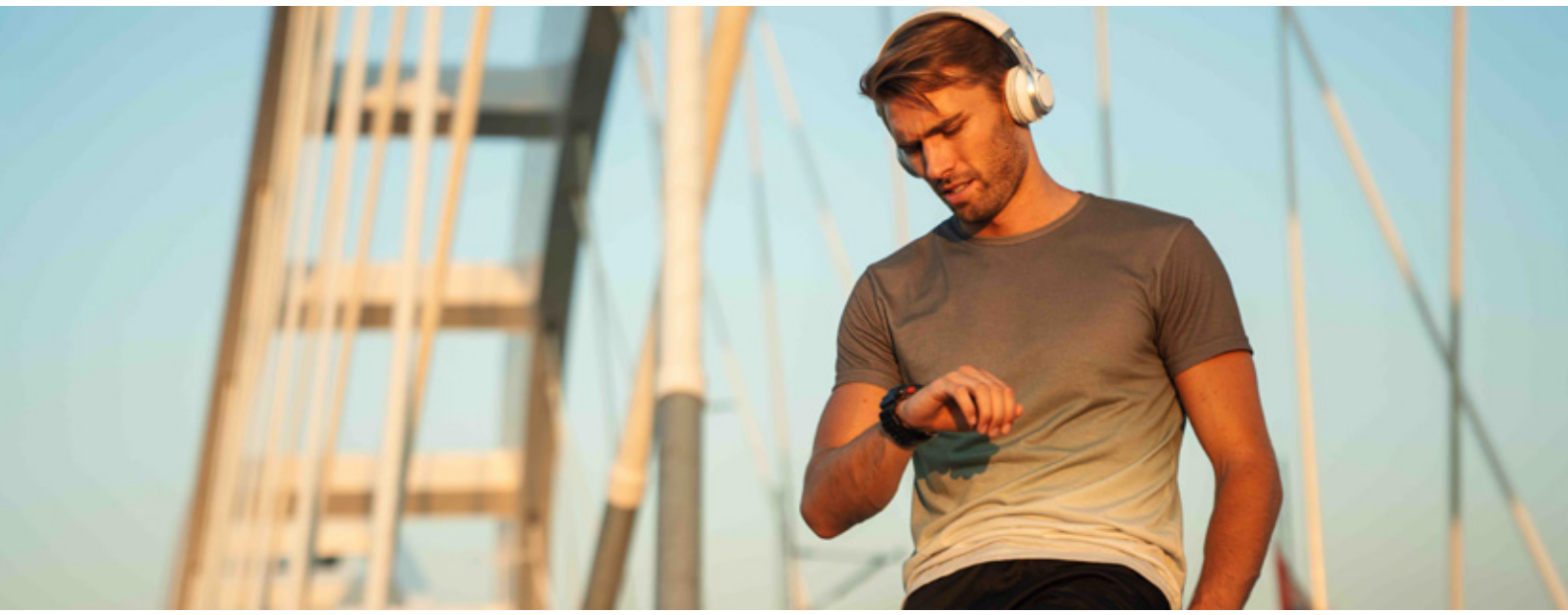


Safety
Freedom from unacceptable risk

Security
The quality or state of being secure (free from danger)

Prior to the use of IoMT medical devices, the matter of safety and effectiveness were more prevalent than the matter of security. However, today security is considered an explicit requirement of patient safety. For example, a cyber criminal could re-program a wirelessly connected and controlled pacemaker - causing cardiac arrest to the patient. This is an example of a security risk with a safety impact. The security lies with the data being transmitted and controlled, while the safety lies in the end impact to the patient. The sensitivity of the data stored within medical devices can also result in incorrect diagnoses and improper, failed, or delayed treatment.

Since PHI is associated with high data security risks, healthcare organizations have to comply with security regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in North America or the General Data Protection Regulation (GDPR) in Europe. There are other cybersecurity preparedness regulations and requirements that should also be observed and managed for an organization to demonstrate its cybersecurity preparedness.



15%

RISE IN BREACHES OVER THE PAST THREE YEARS

$4.45 MILLION

AVERAGE COST OF A BREACH ACROSS ALL INDUSTRIES GLOBALLY

$11 MILLION

AVERAGE COST OF A HEALTHCARE BREACH - MOST COSTLY ACROSS ALL INDUSTRIES

Case studies

SELECT RECALLS & BREACHES IN THE HEALTHCARE INDUSTRY

$100–$50,000

FINES PER PATIENT RECORD LOST OR COMPROMISED RESULTING FROM HIPAA VIOLATIONS

MEDICAL DEVICE RECALLS

Date and organization	Scale of recall	Potential damages	Remediation
April 2023 A corporation operating in more than 140 countries that specializes in sequencers, diagnostic and research genomics.	Class II Recall: 1,014 sequencers	• Potential for unauthorized access due to lack of security controls • Hackers could take control remotely and alter configurations and genomic data • Faulty results or a full data breach	• Downloadable software patch
August 2018 – October 2021 A medical device company with reported revenues of $31 billion that operates in more than 150 countries.	Class I Recall: 31,310 remote-controlled insulin pumps	• Potential for unauthorized access due to a lack of security controls • Hackers could record and replay communication between remote and pump • Ability to alter insulin dosage or halt delivery • Potential for serious health implications or death	• Replacement of all affected devices • Shipment costs to recall and return devices to healthcare facilities/patients

HEALTHCARE SERVICE PROVIDER BREACHES

Date and organization	Scale of breach	Threat vector	Damages and compromised data	Remediation and next steps
July 2023: A for-profit operator of more than 2,100 healthcare facilities and hospitals.	11 million patients	Unauthorized access from laptop at external location	• Names • Contact info • Birth date • Gender • Appointment dates and locations	• 4 class action lawsuits • Complaints in suits contend that service provider violated its duty of care to protect data and did not employ reasonable measures to protect private information
February – March 2023: Largest American insurer of government-sponsored dental plans for seniors and children.	8.8 million patients	Malware and Ransomware	• Systems infected with malicious code • Unauthorized access to systems that removed copies of PHI, including those of children	• Service provider refused to pay $10 million ransom • As a result, all files posted to the dark web
December 2022 – February 2023: One of the largest managed health networks in the Southern United States.	3.3 million patients	Malware via phishing (email)	• Names • Addresses • Birthdate • SSN • Diagnosis and treatment • Lab results • Prescription data • Radiology reports	• At least 11 lawsuits • $100 - $3,000 per class member
December 2022: A focused, women's healthcare service provider.	4.1K patients	Access through third-party technology partner	• Radiology and ultrasound apps were rendered inaccessible	• Backup sources and restoration measures remedied some lost data • Electronic Medical Records from April - December 2022 were not retrievable or recoverable; data permanently lost

*Sources for case studies can be provided upon request.

Cybersecurity preparedeness regulations

Between countries and geographic jurisdictions, cybersecurity preparedness regulations and requirements for medical devices differ. In fact, regulations for securing medical devices often overlap with industry-focussed data privacy regulations or broader cybersecurity regulations. Many geographies have adopted broad cybersecurity regulations that cover data privacy, including data privacy with respect to patient data. For example, HIPAA in the United States and Canada governs the collection of health information. This would be of relevance to any organization with products or services that intend to store patient data from these geographic markets.

In the European Union (EU), the broader GDPR is designed to enhance the privacy and security of data across many industries, including healthcare. GDPR governs the collection, use, transmission, and security of data collected from residents of any of the 28 member countries of the EU. The law applies to all EU residents, regardless of the organization's location that collects the personal data. As such, medical device data privacy regulations and GDPR overlap in many areas.

Organizations can choose to secure their devices to a standard that is adequate to facilitate healthcare services or sell devices internationally.

FDA & CYBERSECURITY OF MEDICAL DEVICES

The U.S. Food and Drug Administration (FDA) regulates medical devices to ensure their safety and effectiveness. For every medical device with software, cybersecurity is checked during the Pre-Market Approval, De Novo, or 510(k) submission regulatory pathways. In 2022, draft cybersecurity Quality Management System (QMS) and premarket submission guidelines were also published to replace the 2018 version of the guideline that puts more emphasis on Total Product Life Cycle (TPLC). Although these guidelines are not legally binding, if you can show your cybersecurity preparedness through an official certification, this may help with your FDA approval.

Developers and manufacturers are responsible for the testing and re-validation of their technology and devices. The FDA evaluates that these tests were carried out, supported by documented evidence. Companies that manufacture software used in medical devices from external parties (software of unknown provenance) are also responsible for validating its secure use in medical devices.[7]

GLOBAL DATA PRIVACY & MEDICAL DEVICE CYBERSECURITY REGULATIONS

Below are countries or jurisdictions that have adopted cybersecurity or data privacy regulations at the national level, or where regulations at this level are in discussion. For select markets, well-defined medical device cybersecurity regulations have also been included.

ARGENTINA

Personal Data Protection Act

AUSTRALIA

Privacy Act

BRAZIL

General Law for the Protection of Personal Data (LGPD)

Resolution for Regulation of Software as a Medical Device (SaMD)

CANADA

Canada's Consumer Privacy Protection Act (CPAA)

Pre-market Requirements for Medical Device Cyber Security

CHILE

Personal Data Protection Law (PDPL)

CHINA

Personal Information Protection Law (PIPL)

ECUADOR

Protection of Personal Data

EGYPT

Personal Data Protection Law

EU

General Data Protection Regulation (GDPR)
MDCG 2019-16 Guidance on Cybersecurity for Medical Devices

INDIA

Digital Personal Data Protection Bill

JAPAN

Protection of Personal Information (APPI)

KENYA

Data Protection Act

MALAYSIA

Personal Data Protection Act (PDPA)

NEW ZEALAND

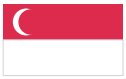
Privacy Act

NIGERIA

Nigeria Data Protection Regulation (NDPR)

RUSSIA

Federal Law on Personal Data (FDL)



SINGAPORE

Personal Data Protection Act (PDPA)

SOUTH AFRICA

Protection of Personal Information Act (POPI)

SOUTH KOREA

Personal Information Protection Act (PIPA)

SWITZERLAND

Federal Act on Data Protection (aligned with GDPR)

THAILAND

Personal Data Protection Act (PDPA)

UGANDA

Data Protection and Privacy Act

UNITED STATES

Cybersecurity in Medical Devices: Quality Systems Considerations and Content of Premarket Submissions

FD&C Act – Ensuring Cybersecurity of Medical Devices

URUGUAY

Data Protection Act Law

In 2020, the International Medical Device Regulators Forum (IMDRF) produced a useful global reference built upon a unanimous understanding of challenges and solutions with respect to the cybersecurity of medical devices.

ISO/IEC 27001: An ISMS governance framework

What are ISO and IEC?

International Organization for Standardization (ISO) is a global, non-profit organization that represents 160 countries through a single standards body for each country. ISO delivers credibility through the implementation of internationally recognized best practices. It is a great place to begin – or to continue - maturing your information security environment.

The International Electrotechnical Commission (IEC) provides a standardized approach to testing and certification. IEC testing brings together the agreed-upon set of rules, specifications, and terminology that allow manufacturers to have their devices tested for conformity.

ISO and IEC Joint Technical Committee (JTC 1) for information technology, is a consensus-based, voluntary international standards group that determines best practices as they relate to IT standards and communications.

A HOLISTIC APPROACH TO MANAGING INFORMATION SECURITY RISK

ISO/IEC 27001 can equip medical device manufacturers and suppliers with a governance framework that specifies the requirements that are needed to establish, implement, maintain, and continually improve an Information Security Management System (ISMS), including its cybersecurity component. It includes requirements for assessing and treating information security risks and prioritizing cyber threats, to benefit your operations as well as to meet the expectations of your customers and partners.

Certification also confirms that your organization is fulfilling its cybersecurity and privacy requirements to the requirements of an internationally recognized standard, providing a solid foundation for fulfilling legal and regulatory requirements. ISO/IEC 27001 certified organizations can demonstrate the integrity of their data and systems, and commitment to information security, cybersecurity, and privacy protection.

Key to data protection within the ISO/IEC 27001 certification is ensuring data confidentiality, integrity and accessibility - the "CIA Triad". It promotes vital security features that enable and ensure operational continuity and data protection for all data under your organization's control and – where applicable – for the design, manufacturing, and operation of a given medical device. It starts from implementation within and moves outwards to cover data security considerations within the supply chain.

Confidentiality
Data is only available to the parties that it is intended for.

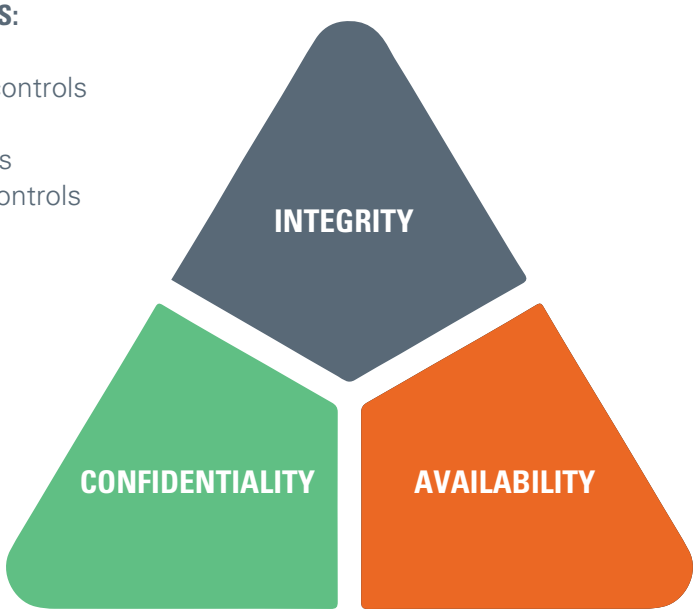
Integrity
Data is not modified against the will of the data holders.

Availability
The data is reliably available to users and will not be lost.

BASED ON THE CIA TRIAD, ISO/IEC 27001 COVERS:

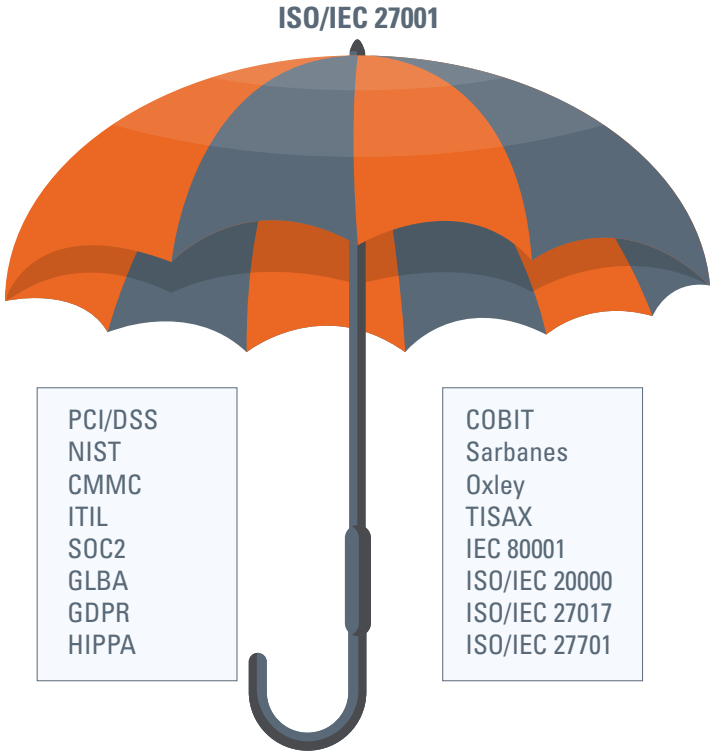
- Organizational controls
- People controls
- Physical controls
- Technological controls

CIA TRIAD



INDUSTRY-AGNOSTIC APPROACH WTH GLOBAL COVERAGE

As a governance structure, it also covers numerous critical standards that your business might be expected to comply with. For example – GDPR for privacy protection, PCI/DSS for credit card processing, HIPAA for the healthcare industry. With its industry-agnostic approach, organizations across a range of commercial sectors are served well by the ISO/IEC 27001 certification. In fact, it is the foundation for other standards within the 27001 series.



ISO/IEC 27001 STRUCTURE

Because it is an international management system standard, it aligns and can be integrated with other globally recognized standards.

This alignment allows you to implement the requirements of several of these standards within your organization with minimal effort.

- ISO/IEC 27701 (Privacy Management)
- ISO 22301 (Business Continuity)
- ISO 9001 (Quality)
- ISO 14001 (Environmental)
- ISO 45001 (Occupational Health and Safety)

PINPOINT VULNERABILITIES IN YOUR ORGANIZATION & SUPPLY CHAIN

A vulnerability is defined in ISO frameworks as "a weakness of an asset or control that can be exploited so that an event with a negative consequence occurs."

An ISO/IEC 27001 certification includes a detailed risk assessment that enables your organization to pinpoint risks and implement security that suits your unique business requirements. It also sets the foundation for the continual review and refinement of processes, delivering a long-term security roadmap for data protection.

An asset is anything of value to an organization, whether tangible (laptops, servers etc.) or intangible (intellectual property, patient records etc.).

In October 2022, the standard was updated to reflect the evolution of business practices such as remote working and how controls should be mapped for different stakeholders, including remote employees. In fact, the primary reason for the update was to recognize the importance of including cybersecurity and privacy in an IT governance framework.

Critical areas of IT vulnerability

Besides the already mentioned technical aspects, it is worthwhile to emphasize that the human element is a key factor in enabling the access and compromise of data through any of these areas of vulnerability.[8] This is why an information security governance framework also places importance on the training and education of an organization's employees, to ensure that staff are cognizant of potential threats and are able to recognize or avoid them. ISO/IEC 27001 ensures that you are vetting your people, your policies, and your technology.

Any information management system that is implemented to this standard is a tool for risk management, cyber-resilience, and operational excellence.

Business & financial benefits of certification

Certification is evidence of an independent review of your effective implementation of a robust ISMS, based on globally recognized best practices. This provides assurance to clients and to business partners that your organization takes information security, cybersecurity, and privacy seriously. At the same time, your organization gains a holistic view of its information security posture and gains the important ability to be proactive in the face of cybersecurity threats, rather than reactive. Security, regulatory and business

continuity requirements can now operate under a single framework, mapping to each other. This eliminates redundancies and the cost of maintaining multiple management systems and associated audits. It also reduces the frequency at which audits need to be conducted; this alone often offsets the cost of becoming certified. The direct and indirect business and financial benefits that stem from an ISO/IEC 27001 certification are numerous.

Greater internal awareness of information security and cybersecurity within the organization, from employees to C-suite; better prevention of human error as a trigger for a security breach.

Enhanced information security processes improve organizational efficiencies through optimized workflows, streamlined efforts, and optimized resource allocation; organizations mature their information security posture.

Enhanced preparedness minimizes data loss and reputational damage; a disaster recovery plan supports data recovery and minimizes revenue loss from downtime in the event of a security breach.

Greater business opportunities with security-conscious customers; ability to gain status as a preferred supplier and to access markets or industries that require demonstration of implemented cybersecurity measures.

Enhanced cybersecurity and privacy measures mitigate the likelihood of a successful data breach; this in turn mitigates major financial loss associated with incident response, remediation, legal proceedings, and fines or penalties.

Enhanced alignment of legal, regulatory, and contractual information security requirements facilitates a streamlined approach to maintaining compliances; better ability to comply with mandatory compliances on time.

How to get certified

ISO/IEC 27001 has a clearly defined and established certification process, including audits and recommendations.

Certification lifecycle

There are seven 'steps' to becoming certified. The gap assessment however is not a requirement, but instead an option for certification. The certification activity really starts before the beginning of the audit. It is imperative for staff across the organization to be trained, a risk assessment performed, and an internal audit conducted. The audit phase begins at Stage 1, ensuring that the system documentation and fundamental processes are in place. If non-conformances are noted during Stage 1, the organization will need to address these before moving on to Stage 2.

Stage 2 is the most intense stage and can include multiple auditors and multiple sites for the audit, depending on the pre-determined scope of the management system. Major non-conformances or minor non-conformances can be identified. In some cases, no non-conformances are found.

Minor non-conformances are instances where the correct process is in place, but it is not producing the right outcomes or is not consistently effective. A major non-conformance is identified when there is a system breakdown or lack of a system. Additional cost and effort may be involved for the remediation of a major non-conformance.

Upon completion of your audit and after the audit report has been reviewed by an independent technical reviewer, your organization will be provided with an ISO/IEC 27001 certificate that can become part of your documentation in response to new RFPs and shared with existing clients. Of course, news of your certification should also be shared across your business network.

Expert auditors

ISO/IEC 27001 auditors are qualified and properly trained to conduct ISO auditing.

Independent certification body

Accredited certification body's processes are monitored and verified by relevant national and international accreditating agencies.

The control framework is relevant

The documented control framework has the capability to address the certification requirements.

POST-CERTIFICATION

Once the organization achieves certification, surveillance audits typically take place once per year. After three years there will be a recertification audit that is similar to the original stage1/stage2 audits. This ensures the continuity of processes and the implementation of enhancements recommended through the initial audit. The surveillance audit also ensures that the organization is consciously working to improve their system for greater efficiency and effectiveness.

As all management systems, ISO/IEC 27001 is industry agnostic - so any developer or manufacturer with the ISO certification can seamlessly work with any organization in the supply chain that is also certified. They can also sell more easily to clients or healthcare service providers who have this certification. Vice versa, healthcare service providers often seek to work with third parties who are certified to operate with greater efficiency and peace of mind.

OTHER RELATED CERTIFICATIONS

These certifications particularly important to medical device developers and manufacturers and are structured similarly to ISO/IEC 27001.

ISO/IEC 27701:2019

Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management

"Specifies requirements and provides guidance for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization. It is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS."

ISO/IEC 22301:2019

Security and resilience - Business continuity management systems

"Specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise. It assesses an organization's ability to meet its own business continuity needs and obligations."

SGS: A trusted partner

SGS is the world's leading testing, inspection and certification company. We can support any organization in the medical device space or healthcare industry with achieving their ISO/IEC 27001 certification.

Example of an SGS ISO/IEC 27001 certificate

Certificate XX/XXXX

The management system of

Company Certified Name

<Address: Company name, street, postcode, country>

has been assessed and certified as meeting the requirements of

ISO/IEC 27001:2022

For the following activities
Scope of accreditation.

This certificate is valid from XX Month XXXX until XX Month XXXX and remains valid subject to satisfactory surveillance audits.
Issue X. Certified since XX Month XXXX.

Authorised by

Accredited Affiliate Name
<Accredited Affiliate Address> (Street name and number, City, Postcode, Country)
t +00 (0) 000-00-00 www.sgs.com

This document is issued by the Company subject to its General Conditions of Certification Services accessible at www.sgs.com/terms_and_conditions.htm. Attention is drawn to the limitations of liability, indemnification and jurisdictional issues established therein. The authenticity of this document may be verified atthttp://www.sgs.com/en/certified-clients-and-products/certified-client-directory. Any unauthorized alteration, forgery or falsification of the content or appearance of this document is unlawful and offenders may be prosecuted to the fullest extent of the law.

Page 1

TRANSITIONING FROM ISO/IEC 27001:2013 TO ISO/IEC 27001:2022

If your organization is already certified to ISO/IEC 27001, this may be the 2013 version of the certification. Moderate efforts will be needed to transition to the new ISO/IEC 27001:2022 version.

These include revising your internal policies in accordance with the new subclauses and modified requirements, as well as the risk assessment results and risk treatment plan in accordance with ISO/IEC 27001:2022 Annex A, and subsequently updating your organization's Statement of Applicability (SoA).

SGS can help you with a smooth transition to ISO/IEC 27001:2022.

WHY SGS?

Whether you are manufacturing MRI machines, intelligent software as a medical device, hip implants, pregnancy tests or thermometers, our assessments are robust and transparent, offering you not just assurance of safety and efficacy, but a competitive edge that comes from demonstrating regulatory trust. Because regulations and standards differ across countries and industries, we have specialists across the world to help ensure your compliance. We can provide audits against recognized certification schemes in North America, the EU, and around the globe.

SGS has been the world's leading certification body for decades, offering a comprehensive range of services to help organizations comply with a host of international, national, regulatory and industry standards, as well as demonstrate best practices. Our global network of expert auditors performs thousands of assessments each year, working confidently with tiny 1-person organizations to large, international organizations. We provide everything you need to achieve best practices, continually improve, and demonstrate that you are a reliable and trustworthy organization.

Our training arm, SGS Academy, also offers broad range of training courses, through a variety of methodologies, including in-person, virtual and e-learning. The Academy courses include introduction, implementation, internal and lead auditor courses as well as transition courses.

SOCIAL RESPONSIBILITY

The UN has created 17 Sustainable Development Goals (SDGs) as an urgent call for action. For each SDG, ISO has identified the standards that make the most significant contributions. Many of the standards contribute to more than one SDG. Download our More Than Just Best Practice and Reassurance – How Our ISO Services Align with the UN SDGs information sheet for more details.

Next steps: Transition or first-time certification

To get started with your ISO/IEC 27001 certification, please reach out to your local SGS team. We can help you transition your existing certification or, if you're starting off, we can help you understand the inter-related certifications and which one best suits your business requirements.

ATTEND OUR VIRTUAL INTRODUCTORY TRAINING COURSE:

ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection - Information Management Systems (ISMS) Introduction Training Course

www.sgs.com

certification@sgs.com

End notes

1
https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

2
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7151197/

3
https://www.chiefhealthcareexecutive.com/view/paying-the-ransom-hospitals-face-hard-decisions-in-cyberattacks-special-report

4
https://www.sec.gov/news/speech/2014-spch061014laa

5
https://www.wsj.com/articles/cybersecurity-tops-the-cio-agenda-as-threats-continue-to-escalate-11666034102

6
https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices

7
https://www.fda.gov/media/71794/download

8
https://www.verizon.com/business/resources/reports/dbir/

WWW.SGS.COM

SGS North America
201 Route 17 North
Rutherford, NJ 07070
United States

WHEN YOU NEED TO BE SURE