Congenius

Congenius Whitepaper

Cybersecurity for medical devices

June 2023
By Paul Gardner

Edited by Hannah Matthews

Contents

Introduction 4

Section 1 | Cybersecurity for medical devices - Life Cycle management 5

i. Legislation & Regulations in the EU & US
ii. Standards
iii. Medical Device Security Risk Management | Identifying, Evaluating, Mitigating, Monitoring & Reassessing Security Risks
iv. Documentation
v. CBOMs / SBOMs

Section 2 | Cybersecurity for the business processes of medical device manufacturers 29

i. Legislation & Regulations in the EU & US
ii. Standards
iii. The benefits of implementing an ISMS
iv. How to implement a compliant ISMS
v. Implementing a compliant ISMS | Effort, Timescales, Maintenance & Certification

Section 3 | Cybersecurity for suppliers to medical device manufacturers 40

Conclusion 43

Guidance links 45

Introduction

Introduction

Medical devices are often connected to networks and can be vulnerable to cyber-attacks, which can compromise patient safety and the confidentiality of patient data.

It's imperative that **medical device manufacturers** implement cybersecurity measures to prevent unauthorised access, ensure data confidentiality, and protect against hacking and other cybersecurity threats. They must also comply with applicable regulations and standards, such as the FDA's premarket review and post-market surveillance requirements.

Business processes are also susceptible to cyber-attacks, which can result in data breaches, financial losses, and reputational damage. To mitigate the risks, organisations must establish cybersecurity policies and procedures, train employees on cybersecurity best practices, and implement technical measures such as firewalls and intrusion detection systems. Conducting regular risk assessments to identify vulnerabilities and implementing appropriate controls is also a necessity.

Suppliers to the legal manufacturer of the medical device may have access to confidential data or be part of the supply chain for critical components of the medical device. Therefore, it is essential to ensure that suppliers also have appropriate cybersecurity controls in place. This includes the vetting of suppliers' security practices, ensuring compliance with security policies and relevant regulatory requirements and standards, as well as monitoring suppliers for potential security breaches.

Cybersecurity is crucial for medical device manufacturers, business processes, and suppliers to the legal manufacturer, and whilst each requires unique consideration, all require the implementation of appropriate controls to protect against cyber threats.

This whitepaper looks at the legislation, regulations, standards, and considerations for stakeholders involved in the cybersecurity of medical device software.

Section 1

Cybersecurity for medical devices | Life Cycle management

Cybersecurity for medical devices | Life Cycle management

Cybersecurity for medical devices refers to the protection of medical devices from cyber threats such as unauthorised access, exploitation, and interference.

These threats can compromise the integrity, availability, and confidentiality of medical devices and the information they process, transmit, or store. Medical devices with connectivity to other devices, networks, or the internet are particularly vulnerable to cyber threats, as they can be accessed and exploited remotely. Examples of medical devices that may be at risk include SaMD Apps, pacemakers, insulin pumps, imaging devices, and electronic medical record systems.

In this section you'll find advice on:

- Legislation & Regulations in the EU & US
- Standards
- Medical Device Security Risk Management
- Documentation
- CBOMs / SBOMs

Cybersecurity for medical devices | Life Cycle management

Legislation & Regulations in the EU

In the European Union, medical devices are regulated under the **Medical Devices Regulation (MDR) 2017 / 745** and the **In Vitro Diagnostic Medical Devices Regulation (IVDR) 2017 / 746**. These regulations include requirements related to cybersecurity, including:

- **General Safety and Performance Requirements** (MDR Article 10 and IVDR Article 10): These articles require medical device manufacturers to ensure that their products are designed and manufactured in a way that ensures their security and protects against unauthorised access.

- **Post-Market Surveillance** (MDR Article 83 and IVDR Article 78): These articles require medical device manufacturers to monitor their products for cybersecurity vulnerabilities and to take appropriate corrective actions if such vulnerabilities are identified.

- **Person Responsible for Regulatory Compliance** (MDR Article 15 and IVDR Article 15): These articles require medical device manufacturers to designate a person responsible for regulatory compliance who is tasked with ensuring that the product meets all applicable regulatory requirements, including those related to cybersecurity.

A note on the General Data Protection Regulation (GDPR)

While GDPR does not specifically address medical device cybersecurity, it does establish requirements for the protection of electronic protected health information. Medical device manufacturers must ensure that their devices comply with GDPR requirements when used in healthcare settings that involve the use or transmission of sensitive data.

Cybersecurity for medical devices | Life Cycle management

Legislation & Regulations in the US

In the United States, the Food and Drug Administration (FDA) has the authority to regulate medical devices, including those that contain software or are connected to the internet. The US government has passed several laws related to cybersecurity and medical devices:

Consolidated Appropriations Act, 2023

The **Consolidated Appropriations Act, 2023**, also known as the **Omnibus Act**, includes a provision in Section 3305 titled "Ensuring Cybersecurity of Medical Devices." This provision requires the FDA to update their guidance on the cybersecurity of medical devices to include specific recommendations for pre-market submissions, post-market submissions, and periodic reporting requirements.

Federal Food, Drug, and Cosmetic Act (FD&C Act)

Section 524B of the **Federal Food, Drug, and Cosmetic Act (FD&C Act)** was updated as a result of Section 3305 of the Omnibus Act. The updated Section 524B now requires medical device manufacturers to develop and implement a plan for disclosing, investigating, and addressing cybersecurity vulnerabilities and exploits in their devices. The updated section also requires manufacturers to submit an annual report to the FDA on the status of their cybersecurity practices and to provide updates to the FDA on any significant cybersecurity incidents. The amendments to Section 524B became effective upon the signing of the Consolidated Appropriations Act, 2023 on 16 March 2023.

Cybersecurity for medical devices | Life Cycle management

Legislation & Regulations in the US (continued)

Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems under section 524B of the FD&C Act

The FDA has recently released guidance entitled **"Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act."** The guidance outlines the agency's expectations for submissions related to the cybersecurity of medical devices and provides details on the FDA's Refuse to Accept (RTA) policy for premarket submissions that do not meet the requirements of Section 524B of the FD&C Act.

The guidance describes the types of information that should be included in premarket submissions to demonstrate compliance with Section 524B, such as a summary of the device's cybersecurity risks, a cybersecurity bill of materials, and a summary of the device's cybersecurity controls. The guidance also provides information on how the FDA will review these submissions, including its process for conducting a cybersecurity review and its expectations for ongoing monitoring and reporting of cybersecurity issues.

The release of this guidance is a significant step forward in the FDA's efforts to address cybersecurity risks in medical devices and to ensure the safety and effectiveness of these devices. It provides manufacturers with clear expectations for demonstrating compliance with Section 524B and for submitting complete and accurate premarket submissions.

Cybersecurity for medical devices | Life Cycle management

Legislation & Regulations in the US (continued)

The 21st Century Cures Act of 2016

This act includes provisions for medical device cybersecurity, requiring the FDA to establish a program for assessing and mitigating cybersecurity risks associated with medical devices. The law also requires medical device manufacturers to implement policies and procedures for vulnerability reporting and remediation.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996

While HIPAA does not specifically address medical device cybersecurity, it does establish requirements for the protection of electronic protected health information (ePHI). Medical device manufacturers must ensure that their devices comply with HIPAA requirements when used in healthcare settings that involve the use or transmission of ePHI.

The FDA has issued several other guidance documents related to cybersecurity in medical devices which are listed in our Guidance Links section at the end of this whitepaper.

These laws, along with the guidance documents, form a comprehensive regulatory framework for medical device cybersecurity in the US. The specific requirements and implementation details of each law may differ, but the general goal is to ensure the safety and security of medical devices and protect patients and healthcare providers from cybersecurity threats.

Cybersecurity for medical devices | Life Cycle management

Standards

There are several standards that apply to the cybersecurity of medical devices. The specific standards that apply may vary depending on the type of device and the regulatory requirements in the country or region where the device is marketed.

Some of the commonly recognised standards for the cybersecurity of medical devices include:

ANSI/AAMI SW96:2023 - Standard for Medical Device Security - Security Risk Management for Device Manufacturers

This standard provides requirements on methods to perform security risk management for a medical device in the context of the safety risk management process required by ISO 14971, and the document is intended to be used in conjunction with AAMI TIR57 and AAMI TIR97.

ISO 14971:2019 - Medical devices - Application of risk management to medical devices

This standard provides guidance on the application of risk management to medical devices, including cybersecurity risks.

IEC 62304:2006/Amd 1:2015 - Medical device software - Software life cycle processes

This standard provides a framework for the development and maintenance of medical device software, including cybersecurity considerations.

Cybersecurity for medical devices | Life Cycle management

Standards (continued)

NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations

This is a set of security and privacy controls developed by the National Institute of Standards and Technology (NIST) that can be used to manage cybersecurity risks for medical devices in the US.

UL 2900 - Standard for Software Cybersecurity for Network-Connectable Products

This standard provides a framework for assessing the cybersecurity of network-connected products, including medical devices.

IEC 62443 - Industrial communication networks - Network and system security

This standard provides guidance on the cybersecurity of industrial control systems, which are increasingly being used in medical devices.

It's important to note that these are not the only standards that may apply to the cybersecurity of medical devices. The specific standards that apply may vary depending on the country or region where the device is marketed, and manufacturers should consult with the regulatory authorities in these countries or regions to determine the specific standards that apply to their device.

Cybersecurity for medical devices | Life Cycle management

Medical Device Security Risk Management

Security and safety risk management are two distinct but interrelated approaches to managing risks associated with medical devices. **Security risk management** focuses on minimising the risks of unauthorised access or misuse of the device's data or functions while **safety risk management** focuses on minimising the risks of physical harm or injury to patients caused by the device.

Here's a practical approach to **security risk management** for medical devices:

Identify security risks

The first step in security risk management is to identify potential security risks associated with the medical device. This includes analysing the device's software and hardware components, as well as the ways in which the device is used and connected to other systems.

Evaluate the risks

Once the security risks have been identified, the next step is to evaluate the likelihood and potential impact of each risk.

Mitigate the risks

After evaluating the risks, the third step is to develop and implement mitigation strategies to minimise the risks. This may include modifying the device's software or hardware, implementing access controls, or developing incident response plans.

Monitor & reassess

Security risks are constantly evolving, so it's important to continuously monitor and reassess the risks associated with the medical device. This may involve regular vulnerability assessments, penetration testing, and other security assessments.

Cybersecurity for medical devices | Life Cycle management

Medical Device Security Risk Management (continued)

In comparison, here's a practical approach to **safety risk management** for medical devices:

Identify safety risks

The first step in safety risk management is to identify the potential safety risks associated with the medical device. This includes analysing the device's design, intended use, and potential hazards.

Evaluate the risks

The next stage after identifying the safety risks is to assess the likelihood and potential consequences of each risk.

Mitigate the risks

After evaluating the risks, the third step is to develop and implement mitigation strategies to minimise the risks. This may include modifying the device's design, implementing safety features, or developing warnings and instructions for use.

Monitor & reassess

Safety risks are also constantly evolving, so it's important to continuously monitor and reassess these risks too. This may involve post-market surveillance, adverse event reporting, and other safety assessments.

Cybersecurity for medical devices | Life Cycle management

Medical Device Security Risk Management (continued)

Guidance, such as TIR57, recommends separating the security and safety risk management processes.

This is a sensible recommendation, as the people involved in the processes are not necessarily the same individuals - data security and clinical safety concepts are not managed by the same people with the same qualifications.

For small businesses, this separation could be theoretical. The same people may be managing both processes, without a marked separation of activities on a day-to-day basis. However, the processes should be documented separately. Small businesses may require consultancy from security experts to help manage security risks.

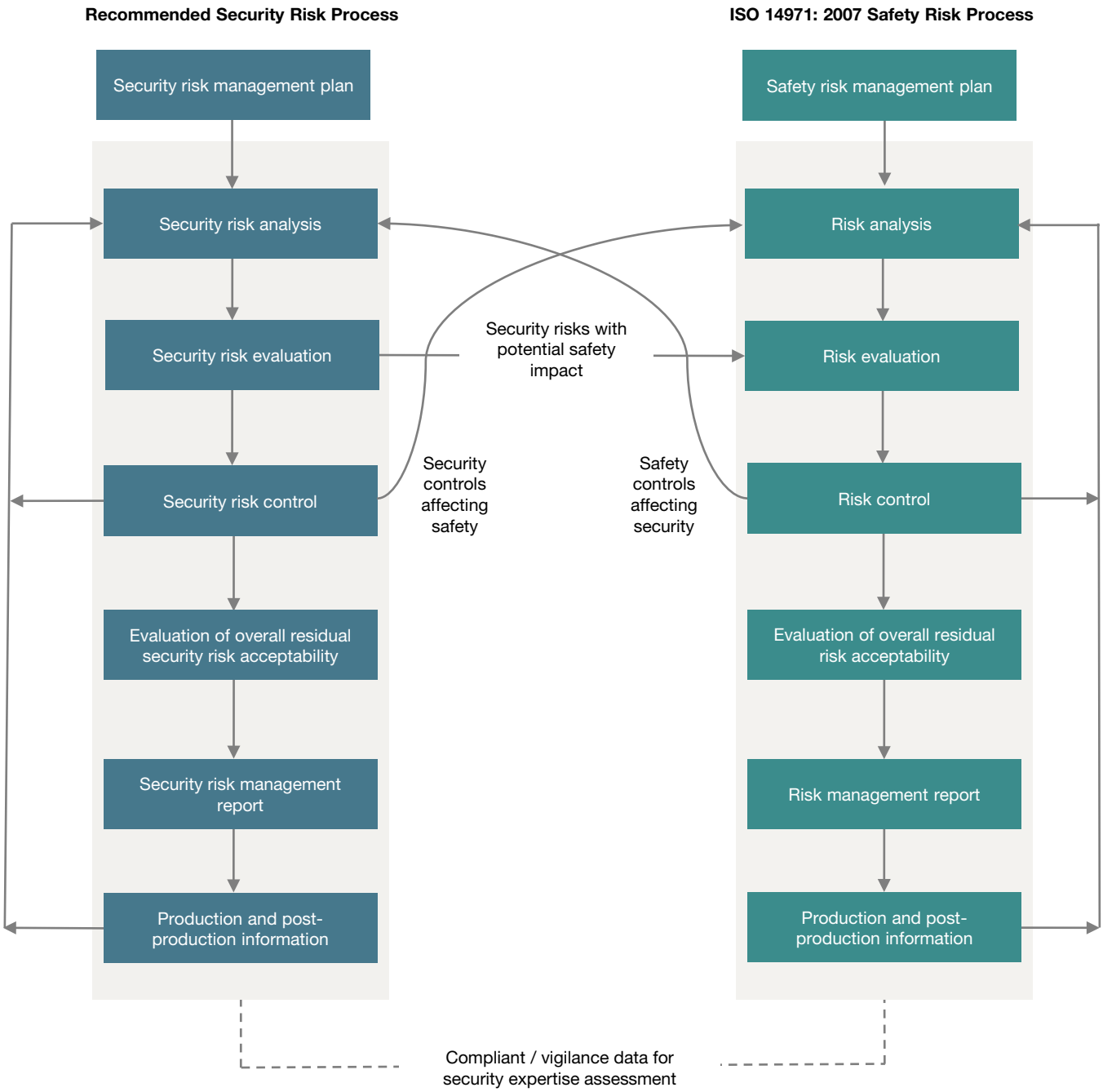
For larger companies, the separation is more practical - with budgets available for maintaining two processes and the necessary qualified persons.

The benefits of separating the processes

Separating the processes is a good way to efficiently monitor security risk management. Keeping a security risk management file separated from the safety risk management file allows for documenting the outputs of the processes without mixing concepts of security risk management (threats, vulnerabilities, assets, adverse impacts), with concepts of safety risk management (hazardous phenomenon, hazardous situation, hazard, harm).

Cybersecurity for medical devices | Life Cycle management

Medical Device Security Risk Management (continued)



The diagram above, extracted from TIR57, shows the interfaces between both processes. In summary, both security and safety risk management are critical components of medical device development and deployment. While the approach to each may differ, the overall goal is to minimise the risks associated with the device to ensure patient safety and security.

Cybersecurity for medical devices | Life Cycle management

Medical Device Security Risk Management | Identifying Security Risks

There are various methods and tools that can be used to identify security risks in medical devices. Here are some examples:

Threat modelling

Threat modelling is a structured approach to identifying potential security threats to a system or device. It involves identifying potential attackers, their motivations and capabilities, and the vulnerabilities of the device. This can be done using tools such as STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) and DREAD (Damage, Reproducibility, Exploitability, Affected users, Discoverability).

Vulnerability assessments

Vulnerability assessments involve identifying and testing the vulnerabilities of a device, including software and hardware vulnerabilities. This can be done using tools such as Nessus, OpenVAS, and Qualys.

Penetration testing

Penetration testing involves simulating a real-world attack on the device to identify potential security weaknesses. This can be done using tools such as Metasploit and Burp Suite.

Cybersecurity for medical devices | Life Cycle management

Medical Device Security Risk Management | Identifying Security Risks (continued)

Code review

Code review involves examining the source code of the device to identify potential security vulnerabilities. This can be done manually or using automated tools such as SonarQube and CodeSonar.

Risk assessment

Risk assessment involves analysing the potential impact of a security breach on the device and its users. This can be done using tools such as FAIR (Factor Analysis of Information Risk) and PRAM (NIST Privacy Risk Assessment Methodology).

Security testing standards

Various security testing standards exist to aid the identification of security risks in medical devices. Examples include IEC 62304, which outlines the software development lifecycle for medical devices, and IEC 80001, which provides guidance on the management of IT networks within healthcare facilities.

It's important to note that these methods and tools are not exhaustive, and each approach may have its limitations. Combining multiple approaches can provide a more comprehensive understanding of the security risks associated with a medical device.

Cybersecurity for medical devices | Life Cycle management

Medical Device Security Risk Management | Evaluating Security Risks

Once potential security risks have been identified in a medical device, the next step is to evaluate and prioritise those risks. Here are some examples of methods and tools that can be used to evaluate security risks in medical devices:

Risk matrix

A risk matrix is a commonly used tool for evaluating risks in medical devices. It involves plotting the likelihood and severity of each risk on a grid to determine its overall risk level. This can be done using tools such as Excel, or specialised risk management software.

Common Vulnerability Scoring System (CVSS)

CVSS is a framework used to evaluate the severity of vulnerabilities in software systems. It assigns a score based on factors such as exploitability, impact, and complexity. CVSS scores can be used to prioritise remediation efforts for identified vulnerabilities.

Attack tree analysis

Attack tree analysis involves breaking down potential security threats into smaller, more manageable components to determine the likelihood and impact of an attack. This can be done using tools such as the Attack Tree Toolkit.

Cybersecurity for medical devices | Life Cycle management

Medical Device Security Risk Management | Evaluating Security Risks (continued)

Quantitative risk analysis

Quantitative risk analysis involves using statistical models to determine the likelihood and impact of each identified security risk. This can be done using tools such as the Monte Carlo simulation.

Checklists & standards

Various checklists and standards exist to aid in the evaluation of security risks in medical devices. Examples include the ISO 14971 standard for risk management, and the NIST Cybersecurity Framework.

It's important to consider that each evaluation method and tool has advantages and disadvantages, and different approaches may be better suited to different types of security risks. To effectively evaluate and prioritise security risks in medical devices, a combination of approaches may be required.

Cybersecurity for medical devices | Life Cycle management

Medical Device Security Risk Management | Mitigating Security Risks

Once potential security risks have been identified and evaluated in a medical device, the next step is to mitigate them. Here are some examples of common approaches to mitigating security risks in medical devices:

Secure design

Implementing secure design principles during the development phase of your device can help prevent the emergence of security vulnerabilities. Secure design includes practices such as code reviews, testing, and the use of secure development frameworks such as the OWASP Secure Coding Practices or the Microsoft Security Development Lifecycle (SDL).

Encryption

Encrypting sensitive data and communications can help prevent unauthorised access or interception. Encryption can be implemented at various levels, including device-level encryption, network-level encryption, and application-level encryption.

Access controls

Implementing access controls such as user authentication, role-based access control, and permissions can limit the scope of potential security breaches by restricting access to sensitive data and functions.

Cybersecurity for medical devices | Life Cycle management

Medical Device Security Risk Management | Mitigating Security Risks (continued)

Monitoring & logging

Implementing monitoring and logging mechanisms can help detect and respond to security breaches in a timely manner. This includes monitoring for suspicious activity, generating alerts, and logging system events for analysis.

Regular updates & patching

Regularly updating and patching your device can help address known security vulnerabilities and prevent the exploitation of these vulnerabilities.

Physical security

Implementing physical security measures such as locks, access controls, and surveillance cameras can help prevent unauthorised physical access to your device.

User training & awareness

Providing user training and awareness programs can help educate users on how to use the device securely and recognise potential security threats.

It's important to note that these mentioned approaches are not exhaustive, and the specific approach to mitigating security risks in a medical device will depend on the nature of the device and the identified risks. For security threats in medical devices to be properly mitigated, a combination of strategies could be required.

Cybersecurity for medical devices | Life Cycle management

Medical Device Security Risk Management | Monitoring & Reassessing Security Risks

Here are some examples of common approaches and tools / frameworks that can be used to monitor and reassess security risks in medical devices:

Vulnerability scanning

Vulnerability scanning tools such as Nessus or Qualys can be used to periodically scan medical devices and identify potential vulnerabilities.

Penetration testing

Penetration testing can be conducted to assess the effectiveness of security controls and identify potential vulnerabilities that may be missed by automated scanning tools.

Threat modelling

Threat modelling can be used to identify potential security threats and prioritise security controls accordingly.

Security assessments

Regular security assessments should be conducted to assess the overall security posture of your medical device and identify areas for improvement.

Cybersecurity for medical devices | Life Cycle management

Medical Device Security Risk Management | Monitoring & Reassessing Security Risks (continued)

Compliance monitoring

Compliance monitoring tools such as Security Information and Event Management (SIEM) can be used to monitor for compliance with security regulations and identify any deviations from expected security behaviour.

Incident response planning

Incident response plans should be developed and regularly reviewed to ensure that they are up-to-date and effective in responding to potential security incidents.

Continuous monitoring

Continuous monitoring of the medical device can be achieved using network monitoring tools such as Intrusion Detection Systems (IDS) or Security Information and Event Management (SIEM) solutions.

It's crucial to remember that these are merely examples and that the precise strategy, tools, and frameworks chosen will depend on the characteristics of your device and the risks determined. To efficiently track and re-evaluate security threats, a variety of techniques may be required.

Cybersecurity for medical devices | Life Cycle management

Documentation

The documentation required to demonstrate compliance for the cybersecurity of medical devices varies depending on the specific regulatory requirements that apply to the device and the jurisdiction in which it is marketed. Some of the common types of documentation that may be required include:

Cybersecurity Risk Management Plan

This plan should detail the methodology used to identify, assess, and manage cybersecurity risks for your device, including details on the types of cybersecurity vulnerabilities that were considered, and any measures taken to reduce or eliminate these risks.

Cybersecurity Design Control Documentation

This documentation should demonstrate how cybersecurity was incorporated into your device's design and development process. This includes design input and output documents, as well as verification and validation protocols and reports. The technical documentation should include information about the device's cybersecurity features, including any cybersecurity measures implemented to reduce the risk of cybersecurity threats. It should also include information about your device's software, including its architecture, interfaces, and potential cybersecurity vulnerabilities.

Cybersecurity Verification Testing

This testing should demonstrate that the device's cybersecurity controls have been implemented correctly, and that they are effective in reducing the risk of cybersecurity threats.

Device Labelling / Instructions for Use

The device labelling should clearly indicate any cybersecurity features, precautions, or limitations that are relevant to the use of the device.

Cybersecurity for medical devices | Life Cycle management

Documentation (continued)

Device Security Updates

The manufacturer should have a process for providing software updates and patches to address cybersecurity vulnerabilities that are discovered after the device has been marketed. The manufacturer should document these updates and make them available to users.

Post-Market Surveillance

The manufacturer should have a process for monitoring the cybersecurity of the device after it has been marketed, and for reporting any cybersecurity incidents or issues that arise.

Incident Response Plan

The manufacturer should have an incident response plan in place that outlines the steps to be taken in the event of a cybersecurity incident or breach involving the device.

Compliance documentation

This includes documentation that demonstrates how the device complies with the relevant regulatory requirements for cybersecurity. This may include conformity assessment reports, certification documentation, and regulatory filings.

The specific documentation required may vary depending on the risk level of the device, the intended use of the device, and other factors. Manufacturers should consult with the relevant regulatory authorities to determine the specific requirements for their device.

In addition to these types of documentation, it’s important to maintain accurate and up-to-date records of any changes or updates to your device's cybersecurity over its lifecycle. This can include documentation related to software updates, security patches, and other changes to the device's design or operation that could impact its cybersecurity.

Cybersecurity for medical devices | Life Cycle management

CBOMs & SBOMs

CBOM and SBOM are two different types of Bill of Materials (BOM) used in the context of cybersecurity for software and hardware components.

CBOM stands for "Component Bill of Materials". It is a list of all the software and hardware components that are used in a particular product. A CBOM is useful for identifying vulnerable components in a product and assessing the risk associated with those vulnerabilities. CBOM can help manufacturers, vendors, and other stakeholders to track the origin of each component and ensure that it meets security requirements.

SBOM stands for "Software Bill of Materials". It is a specific type of CBOM that only includes the software components used in a product. SBOM is important for managing the security of software components in a product. It provides a detailed list of all the software components used in a product, including any open-source or third-party components. This information can be used to identify vulnerabilities and potential risks associated with the software components used in a product.

Both CBOM and SBOM are important tools for managing the security of products. They can help to identify vulnerabilities, assess risk, and track the origin and security of components. Many organisations, including the FDA, are encouraging the use of SBOMs as a best practice for managing the security of software components in medical devices.

Cybersecurity for medical devices | Life Cycle management

CBOMs & SBOMs (continued)

There are various tools available that can help create CBOMs and SBOMs for medical devices. Here are some examples:

National Institute of Standards and Technology (NIST) Cybersecurity Framework	A framework providing guidance for creating a CBOM and managing cybersecurity risks for medical devices.
Common Vulnerability Scoring System (CVSS)	A standardised system for assessing the severity of security vulnerabilities, which can be used to identify and prioritise potential vulnerabilities in a medical device CBOM.
Software Bill of Materials (SBOM) Framework	A framework developed by the National Telecommunications and Information Administration (NTIA) that provides guidance on creating and using SBOMs for software and hardware components.
Open-Source Security Foundation (OSSF)	The foundation offers several tools and resources to help organisations manage cybersecurity risks for open-source software components, including the creation of SBOMs.

Section 2

Cybersecurity for the business processes of medical device manufacturers

Cybersecurity for the business processes of medical device manufacturers

In this section you'll find advice on:

- Legislation & Regulations in the EU & US
- Standards
- The benefits of implementing an ISMS
- How to implement a compliant ISMS
- Implementing a compliant ISMS | Effort, Timescales, Maintenance & Certification

Cybersecurity for the business processes of medical device manufacturers

Legislation & Regulations in the EU

The NIS2 Directive

The NIS2 (Network and Information Systems 2) directive is legislation by the European Commission aimed at enhancing the security of network and information systems across the EU.

The directive builds on the existing NIS Directive, which was adopted in 2016 and has been implemented in all EU member states. The NIS2 Directive was adopted by the European Parliament and the Council of the EU on 13 December 2021.

The directive replaces the current NIS Directive (2016/1148/EU) and sets new rules and standards to enhance the cybersecurity of critical infrastructure and digital services across the European Union. Moreover, the NIS2 Directive proposes a certification framework for ICT products, services, and processes to ensure they meet the appropriate level of security.

This framework aims to ensure that security measures are properly implemented by digital service providers, including those that provide medical devices and digital health solutions. It also requires the establishment of a European Cybersecurity Certification Framework, which will specify the requirements for cybersecurity certification of ICT products, services, and processes.

Cybersecurity for the business processes of medical device manufacturers

Legislation & Regulations in the EU (continued)

Here is a summary of the main topics within NIS2:

- **Security requirements**: NIS2 requires medical device manufacturers to ensure that their processes meet certain security requirements. The directive proposes that these requirements be based on international standards and best practices.

- **Incident reporting**: NIS2 requires medical device manufacturers to report security incidents to national authorities. The proposed directive also establishes a framework for sharing information about security incidents among member states.

- **Certification**: NIS2 proposes the establishment of a certification framework for medical devices, which would ensure that these products meet certain security requirements.

A note on the General Data Protection Regulation (GDPR)

GDPR establishes requirements for the protection of electronic protected health information. Medical device manufacturers must ensure that their devices comply with GDPR requirements when used in healthcare settings that involve the use or transmission of sensitive data.

Cybersecurity for the business processes of medical device manufacturers

Legislation & Regulations in the US

Federal Trade Commission Act (FTCA) Section 5

The primary law governing cybersecurity in the United States is the Federal Trade Commission Act (FTCA) Section 5. This law prohibits deceptive acts and practices in business, including those related to data security.

Health Insurance Portability and Accountability Act (HIPAA) of 1996

HIPPA established requirements for the protection of electronic protected health information (ePHI). Medical device manufacturers must ensure that their systems comply with HIPAA requirements when used in healthcare settings that involve the use or transmission of ePHI.

Cybersecurity for the business processes of medical device manufacturers

Standards

The NIS and FTCA regulations reference that companies should consider compliance with international standards, and the guidance issued by the European Union Agency for Cybersecurity (ENISA) maps security objectives for several best practice standards:

ISO 22301 – Business Continuity Management System

This standard 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.

ISO/IEC 27001 - Information Security Management Systems

This standard provides a framework for implementing and maintaining an information security management system (ISMS) to manage cybersecurity risks. On the following pages you'll find more information on ISMS implementation.

Cybersecurity for the business processes of medical device manufacturers

The benefits of implementing an ISMS

Here are some benefits of implementing an ISO 27001 compliant ISMS:

Compliance

An ISO 27001 certification will demonstrate compliance with various regulations to regulatory authorities and customers.

Marketing edge

In a competitive market your ISMS will differentiate you in the eyes of potential customers.

Lowered expenses

Information Security is often considered a cost with no apparent pay-off. But reducing your expenses due to incident handling demonstrates clear a financial gain.

Increased organisation

An ISMS requires you to define roles and responsibilities and therefore strengthens your internal organisation.

Essentially, your ISO 27001 compliant ISMS could reap many benefits besides being just another certificate on your wall. In most cases, if you present those benefits clearly, your management will understand and support you.

On the following pages you'll find advice on how to implement a compliant ISMS.

Cybersecurity for the business processes of medical device manufacturers

How to implement a compliant ISMS

Here's a practical approach to implementing an ISO 27001 compliant ISMS:

- ✓ **Obtain Management Support:** The main reason certification projects fail is a lack of management support. Obtaining Management Support sets the project on the right track.

- ✓ **Apply Project Management:** Clearly define what is to be done, who is going to do it and within what timescale.

- ✓ **Define the Scope:** For a large organisation it would be pragmatic to implement an ISMS for part of the organisation initially. For a smaller organisation it's necessary to include the whole company in the scope.

- ✓ **Create the Information Security Policy:** This is the primary internal document in your ISMS. It need not be very detailed but should define the basic requirements for information security in your organisation.

- ✓ **Define the Risk Assessment Process:** Risk assessment is the most complex task in the ISMS project. This step defines the rules for identifying the risks, impacts, and likelihood, and defines the acceptable level of risk.

- ✓ **Perform the Risk Assessment & Identify the Risk Controls:** In this step you carry out the Risk Assessment for the process defined above. This should result in a detailed, comprehensive view of the threats to your organisation's data. By identifying the Risk Controls, you prepare to decrease the impact of the identified risks. In this step you will also document the steps taken and seek approval for any residual risks.

Cybersecurity for the business processes of medical device manufacturers

How to implement a compliant ISMS (continued)

- ✓ **Write the Statement of Applicability:** The purpose of the Statement of Applicability, (or SoA) is to list the Risk Controls and define which are applicable, the reasons for any such decisions, and a description of how the Risk Controls are to be implemented in the organisation. The SoA is the document to use to obtain management authorisation to implement the ISMS.

- ✓ **Write the Risk Control Implementation Plan:** This step defines how the Risk Controls identified and authorised by the SoA are going to be implemented.

- ✓ **Plan the effectiveness monitoring:** Here you define how you are going to measure the ISMS progress and the effectiveness of the security processes and controls.

- ✓ **Implement the Risk Controls:** This step is the most difficult as here you introduce change to your organisation. New policies and procedures may need to be introduced. The next step reinforces this one.

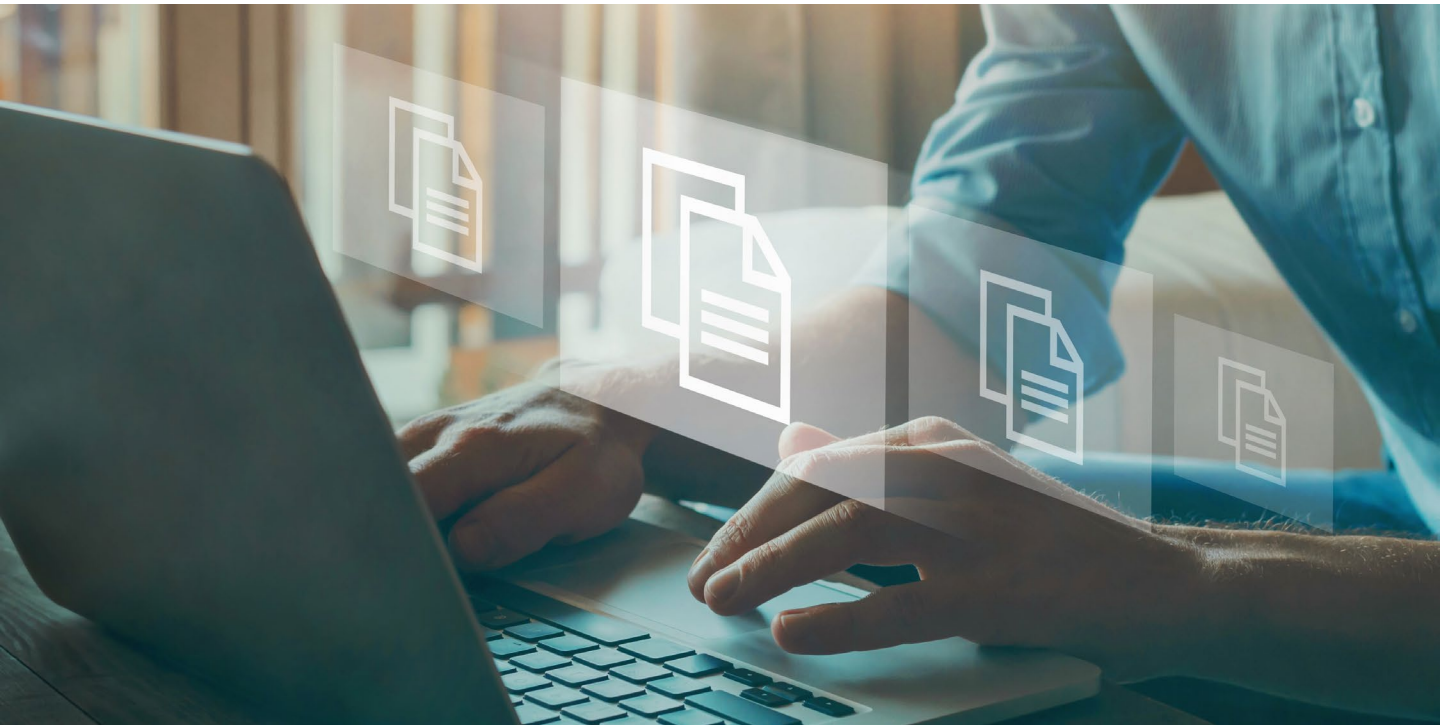
- ✓ **Communication and Training:** To ensure a smoother passage for your proposed changes you need to explain the changes and train your people. The absence of training is a common reason for ISMS project failure.

- ✓ **Operate the ISMS:** This is where your ISMS is used. The generation of records will facilitate the next step.

Cybersecurity for the business processes of medical device manufacturers

How to implement a compliant ISMS (continued)

- ✓ **Monitor the effectiveness of the ISMS:** By reviewing the number and type of incidents you can perform corrective and preventative actions.
- ✓ **Perform Internal Audits:** Through auditing you can also identify corrective and preventative actions.
- ✓ **Carry out a Management Review:** The Management of your company needs to know how the ISMS is performing and must then make any important decisions for improvement.
- ✓ **Make Corrective Actions:** The purpose of the ISMS is to ensure that non-conformities are corrected, or ideally prevented. Therefore, corrective actions are required to be carried out systematically, which means that the root cause of a non-conformity must be identified, and then resolved and verified.



Cybersecurity for the business processes of medical device manufacturers

Implementing a compliant ISMS | Effort, Timescales, Maintenance, & Certification

Implementing an ISMS is not a trivial process. It is complex, time consuming, and requires significant effort. A realistic timescale for a meaningful implementation is two to three months for smaller companies and the process can take over a year for larger organisations.

Your primary effort is expended in planning and executing the **risk assessment** and implementing the **risk controls**.

The duration of implementation for these two phases depends primarily on the size of the organisation:

- Companies of up to 20 employees – up to 3 months
- 20 to 50 employees – 3 to 5 months
- 50 to 200 employees – 5 to 8 months
- More than 200 employees – 8 to 20 months

These times are practical if you involve a knowledgeable consultant. Implementation time can be considerably extended without top management support and / or an experienced project manager.

Work on an ISMS does not stop with the initial implementation; the ISMS needs to be maintained and improved. A good estimate for **maintaining the ISMS is around 25% of the effort for the implementation**.

Finally, to publicly prove that you have complied with ISO 27001, the **certification body will have to undertake a certification audit**. This cost will depend on the size of your company, but for example, in the United States, the certification of a smaller company could be around $7,500.

Section 3

Cybersecurity for suppliers to medical device manufacturers

Cybersecurity for suppliers to medical device manufacturers

As a medical device contract development or manufacturing organisation (CDO / CMO), it is essential to ensure that your suppliers have proper cybersecurity measures in place to protect your intellectual property, customer data, and other sensitive information.

Below and on the following page are some key points to consider regarding cybersecurity for your suppliers:

Require cybersecurity assessments: Before working with any new supplier, require them to undergo a cybersecurity assessment to ensure that they have appropriate security measures in place to protect your company's data.

Install secure communication: Ensure that all communication between your company and suppliers is secure by using encrypted communication channels, such as email encryption or secure messaging platforms.

Protect intellectual property: Make sure that your suppliers have appropriate policies in place to protect your intellectual property. This includes data protection, confidentiality agreements, and non-disclosure agreements.

Insist on employee training: Require that your suppliers provide regular cybersecurity training to their employees to help prevent cyber-attacks.

Cybersecurity for suppliers to medical device manufacturers

Plan for incident response: Make sure that your suppliers have a plan in place for responding to cyber incidents, such as a data breach or ransomware attack.

Require regular updates: Ensure that your suppliers are regularly updating their software and systems to prevent vulnerabilities and patch security holes.

Check compliance with regulations: Check that your suppliers are complying with relevant cybersecurity regulations. If they are a CDO /CMO assess them using section one and / or section two of this document.

All the relevant requirements should be ensured with Quality Agreements established between CDO / CMO and suppliers.

By following these steps, you can help ensure that your suppliers have appropriate cybersecurity measures in place to protect your company's sensitive information.

Conclusion

Conclusion

Effective medical device cybersecurity requires a holistic approach that addresses the entire lifecycle of the device, from design and development to deployment, maintenance, and decommissioning.

This includes implementing secure design principles, conducting risk assessments, implementing appropriate controls and safeguards, and following best practices for secure deployment, management, and decommissioning.

Cybersecurity breaches in the healthcare sector can have serious consequences, including harm to patients, financial losses, and damage to reputation, so it is imperative that medical device manufacturers and healthcare organisations prioritise cybersecurity to both ensure the safety and effectiveness of their devices, and protect the privacy and security of patient data.

Guidance links

Guidance links

EU guidance

Guidance on Cybersecurity for Medical Devices – MDCG 2019-16 (December 2019)

This guidance was issued by the European Commission's Medical Device Coordination Group (MDCG) and provides recommendations for managing cybersecurity risks associated with medical devices in the EU. It includes recommendations for risk management, security controls, and incident management.

US guidance

Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act Guidance for Industry and Food and Drug Administration Staff (March 2023)

This guidance outlines the FDA's expectations for submissions related to the cybersecurity of medical devices and provides details on its Refuse to Accept (RTA) policy for premarket submissions that do not meet the requirements of Section 524B of the FD&C Act.

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff (April 2022)

This guidance provides recommendations to industry regarding cybersecurity device design, labelling, and the documentation that FDA recommends be included in premarket submissions for devices with cybersecurity risk. These recommendations can facilitate an efficient premarket review process and help ensure that marketed medical devices are sufficiently resilient to cybersecurity threats.

NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations - National Institute of Standards and Technology (NIST) (2020)

This is a general guidance document that provides a catalogue of security and privacy controls that can be used to manage cybersecurity risks in any type of information system, including medical devices.

Guidance links

US guidance (continued)

Technical Information Report (TIR) 97: Principles for Medical Device Security – Post-market Risk Management for Device Manufacturers - Association for the Advancement of Medical Instrumentation (AAMI) (2019)

This provides guidance on methods to perform post-market security risk management for a medical device in the context of the safety risk management process required by ISO 14971.

Post-market Management of Cybersecurity in Medical Devices - Final Guidance for Industry and FDA Staff (2016)

This guidance outlines the FDA's recommendations for managing cybersecurity risks associated with medical devices already on the market. It provides recommendations for monitoring, identifying, and addressing cybersecurity vulnerabilities, as well as for communicating with stakeholders about cybersecurity risks.

Technical Information Report (TIR) 57: Principles for Medical Device Security - Risk Management - Association for the Advancement of Medical Instrumentation (AAMI) (2016)

This guidance document provides a framework for managing cybersecurity risks throughout the entire medical device lifecycle. It includes recommendations for risk assessment, vulnerability management, and incident response.

Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software - Final Guidance for Industry and FDA Staff (2005)

This guidance provides recommendations for managing cybersecurity risks associated with medical devices that use off-the-shelf (OTS) software. It includes recommendations for device design, risk assessment, and vulnerability management.

Guidance links

International guidance

Principles and Practices for the Cybersecurity of Legacy Medical Devices IMDRF/CYBER WG/N70 (April 2023)

This guidance document provides stakeholders with clear ways of identifying potential legacy devices and practical, feasible approaches to maintain cybersecurity of legacy medical devices. It provides a variety of options to implement without distorting each jurisdiction's regulatory systems and is intended to be complementary to the IMDRF N60 guidance.

Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity - IMDRF/CYBER WG/N73 (April 2023)

This guidance provides a high-level description of an SBOM and best practices for the generation and use of an SBOM. The purpose of this document is to provide greater detail on the implementation of SBOM and software transparency as relevant to medical device stakeholders, including MDMs, healthcare providers (HCPs), and regulators. In this guidance, healthcare providers include healthcare delivery organisations (HDOs).

Principles and Practices for Medical Device Cybersecurity IMDRF/CYBER WG/N60 (April 2020)

This IMDRF guidance document provides general principles and best practices to facilitate international regulatory convergence on medical device cybersecurity. While the pre-market section primarily addresses medical device manufacturers, the post-market section includes recommendations for all stakeholders.

Guidance links

Standards

ANSI/AAMI SW96:2023 - Standard for Medical Device Security - Security Risk Management for Device Manufacturers

This provides requirements on methods to perform security risk management for a medical device in the context of the safety risk management process required by ISO 14971. The document is intended to be used in conjunction with AAMI TIR57 and AAMI TIR97.

Information Security Management System (ISMS) for Medical Devices - ISO/IEC 27001:2022

This is an international standard that provides a framework for establishing and maintaining an information security management system (ISMS). While not specific to medical devices, this standard can be used by medical device manufacturers to develop an effective cybersecurity management system.

IEC 80001-1:2010 Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities, and activities - International Electrotechnical Commission (IEC) (2010)

This standard provides guidance for managing cybersecurity risks associated with IT networks that incorporate medical devices. It includes recommendations for risk assessment, risk management, and incident management.

Guidance links

Tools & Resources

Cybersecurity in Medical Devices Frequently Asked Questions (FAQs)

This page provides answers to frequently asked questions (FAQs) related to cybersecurity in medical devices.

Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook - Department of Health and Human Services (HHS) (2022)

This document provides guidance for healthcare organisations on how to prepare for and respond to cybersecurity incidents involving medical devices. It includes recommendations for incident response planning, incident detection and reporting, and incident recovery.

Threat Modelling Playbook for Medical Device Cybersecurity

This playbook was developed by the Medical Device Cybersecurity Shared Responsibility Group (MDR-SRG), a collaboration between the medical device industry and the Department of Health and Human Services (HHS) in the United States. It provides guidance on how to apply threat modelling principles to medical devices, including how to identify potential threats, assess their likelihood and impact, and prioritise them based on risk. The playbook is designed to be used by a range of stakeholders, including medical device manufacturers, healthcare providers, and regulatory agencies. It includes a step-by-step process for conducting threat modelling exercises, as well as templates and examples to help organisations get started.

Congenius

Should you have a medical device software cybersecurity challenge, please do get in touch – our eHealth team is ready and happy to help.

Congenius AG
Riedstrasse 1
CH - 8953 Dietikon

E: info@congenius.ch
T: +41 44 741 04 04

congenius.ch

Revision 1 – June 23