Cybersecurity Resource Guide for Healthcare Startups

FERDINAN TUAZON
Graduate Student
San Jose State University
fatuazon@yahoo.com

Abstract — The healthcare sector is no different to any industry in being a target of cyber attacks. Increasing interconnected modern healthcare devices and networks carrying sensitive and private patient data make them prime targets. Healthcare start-ups often with limited resources and cybersecurity expertise are particularly vulnerable in securing their devices. This article takes the key cybersecurity requirements from the US Food and Drug Administration (FDA), the European Union (EU) regulations, and International Medical Device Regulators Forum (IMDRF) documents to create a resource guide for healthcare organizations responsible for designing and developing medical devices at risk of cybersecurity threats. It emphasizes the importance of integrating cybersecurity in the whole product life cycle of a medical device from premarket development until post-market surveillance.

Keywords — Cybersecurity, Healthcare, Start ups, Medical Device, Regulatory

I. Introduction

The advancement of medical technology produces innovative and state of the art medical devices that hugely improve the lives of many patients. Healthcare start-ups have a large part in bringing this advancement to the healthcare industry. With this innovation also comes a significant cybersecurity risk. Healthcare start-ups that usually have limited resources and expertise are vulnerable to these risks. To make sure their devices are secured, they must design and develop their medical devices according to the best cybersecurity practices and standards. Also they must navigate the complex regulatory landscape to meet the requirements to ensure their devices are safe, secured and compliant. In addition, these start-ups must also look at the international regulatory landscape if they want to have their medical devices brought to the global healthcare stage.

Navigating the Regulatory Landscape

US Food and Drug Administration (FDA)

On December 29, 2022, the Consolidated Appropriations Act, 2023 ("Omnibus") was signed into law. Section 3305 of the Omnibus -- "Ensuring Cybersecurity of Medical Devices" -- amended the Federal Food, Drug, and Cosmetic Act (FD&C Act) by adding section 524B, Ensuring Cybersecurity of Devices (section 3305).5 There are several guidance documents of FDA regarding cybersecurity which are non-binding but are recommendation for any manufacturer of medical devices from the premarket submission up to post marketing surveillance.

Premarket Requirements

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions [6]

The FDA guidance document specifies that cybersecurity is part of device safety and the quality system regulation.[6] This section summarizes and covers the key cybersecurity requirements for a premarket submission of a medical device as per US FDA.

1. Secure Product Development Framework (SPDF). An SPDF is a set of processes that help identify and reduce the number and severity of vulnerabilities in products. An SPDF encompasses all aspects of a product's lifecycle; including design, development, release, support, and decommission.6 This includes the following:

   b. Risk Management. The safety and security risks of each device should be assessed within the context of the larger system in which the device operates. Risk management is implemented for the Total Product Life Cycle (TPLC) of the medical device.[6] This includes identification of risks, and vulnerabilities, threat modeling, risk assessment, interoperability considerations, and third-party software components

   c. Software Bill of Materials (SBOM)[6] SBOM supports the inventory and identification of manufacturer and third-party components including various kinds of software. It helps in identifying and assessing the vulnerabilities of each component.

2. Secured Architecture and Design. The US FDA considers different security factors for medical device cybersecurity. These are factors the device should have to implement security measures or objectives. Also the guidance broadly includes all devices even with artificial intelligence (AI) and machine learning, and cloud based services.[6] This includes the following:

   a. Implementation of Security Controls. These are achieved by implementing several security objectives such as:

      - · Authentication
      - · Authorization
      - · Cryptography
      - · Code, Data, and Execution Integrity

- · Confidentiality
- · Event Detection and Logging
- · Resiliency and Recovery
- · Updatability and Patchability[6]

b. Cybersecurity Testing. This includes implementation of security requirements, threat mitigation, vulnerability testing and penetration testing.

3. Transparency. Necessary information regarding the cybersecurity of the medical device should be disclosed to enable users and stakeholders to understand and manage potential threats and vulnerabilities, thereby ensuring the device's safety and effectiveness. This includes proper labeling of the medical device and management plans.

4. Proper Documentation. Proper cybersecurity documentation of the medical device from its design and development must be maintained and complete. Documentation required labeling of the device, security controls and tests implemented during the development, cybersecurity risk considerations including how the medical device will be used and its intended environment, its connection to networks or any other medical and third-party devices. This documentation will help support the device safety and functionality.

Post Market Requirements

Postmarket Management of Cybersecurity in Medical Devices [17]

The security of a medical device does not cease upon the concluding phase of its design and development; it spans the device's total product life cycle. The ever-evolving landscape and advancement of technology consistently bring out novel and more advanced cybersecurity risks and threats. Creating risk management programs and constant monitoring for threats and vulnerabilities will prevent and remediate the risks found within the medical device.

Risk Management Program. Cybersecurity risk management programs should emphasize addressing vulnerabilities, which may permit the unauthorized access, modification, misuse or denial of use, or the unauthorized use of information stored, accessed, or transferred from a medical device to an external recipient, and may result in patient harm.17 These include the following:

a. Monitoring cybersecurity information sources for identification and detection of vulnerabilities and risks

b. Monitoring of third-party software components

c. Verification and validation for software updates and patches

d. Assessment and detection of vulnerability and its impact

e. Processes for vulnerability handling

f. Use of threat modeling to define how to maintain safety and essential performance of a device

g. Adopt a coordinated vulnerability disclosure policy

h. Deploy mitigations that address cybersecurity risk[17]

Some key components of the risk management program are:

1. **Maintaining Safety and Essential Performance.** Manufacturers should define, as part of the comprehensive cybersecurity risk management, their device's safety and essential performance, the resulting severity of patient harm if compromised, and the risk acceptance criteria.17

2. **Assessment of Exploitability of Cybersecurity Vulnerability**. Manufacturers should have a process for assessing the exploitability of a cybersecurity vulnerability.17 Healthcare start-ups can use different tools for vulnerability assessment.

3. **Assessing and Evaluation of Severity of Patient Harm.** Manufacturers should also have a process to assess the severity of patient harm, if the cybersecurity vulnerability were to be exploited.17

4. **Remediation and Reporting.** After risk assessment and evaluation, the manufacturer should implement a remediation and reporting of the vulnerabilities found.

Recognized Standards for Medical Device Cybersecurity

The following standards are recommended and found relevant by FDA in view of cybersecurity for medical devices.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA of 1996

The HIPAA of 1996 establishes federal standards protecting sensitive health information from disclosure without patient's consent.[11]

HIPAA Privacy Rule

The Privacy Rule standards address the use and disclosure of individuals' protected health information (PHI) by entities subject to the rule.[11]

HIPAA Security Rule

The Security Rule protects a subset of information covered by the Privacy Rule. This subset is all individually identifiable health information that a covered entity creates, receives, maintains, or transmits in electronic form.11

National Institute of Standards and Technology (NIST)

NIST Cybersecurity Framework (CSF) 2.0.

The CSF Core Functions — govern, identify, protect, detect, respond, and recover — organize cybersecurity outcomes at their highest level.10

American National Standards Institute/International Society of Automation (ANSI/ISA)

ANSI/ISA 62443-4-1

Security for Industrial Automation and Control Systems – Part 4-1: Secure Product Development Lifecycle Requirements.

The standard emphasizes the importance of defining security requirements, conducting thorough risk assessments and implementing robust verification and validation processes to mitigate potential vulnerabilities.[4]

International Electrotechnical Commission (IEC)

IEC 81001-5-1

Health Software and Health IT Systems Safety, Effectiveness and Security

Part 5-1: Security – Activities in the Product Life Cycle

This document defines the life cycle requirements for development and maintenance of health software needed to support conformance to IEC 62443-4-1 – taking the specific needs for health software into account.[16]

Association for the Advancement of Medical Instrumentation (AAMI)

AAMI TIR57

Principles for Medical Device Security – Risk Management

This Technical Information Report (TIR) provides guidance on methods to perform information security risk management for a medical device in the context of the Safety Risk Management process required by ISO 14971.[1]

International Organization for Standardization (ISO)

ISO 14971

Medical Devices – Application of Risk Management to Medical Devices

This document specifies terminology, principles and a process for risk management of medical devices, including software as a medical device and in vitro diagnostic medical devices.[14]

ISO/IEC 30111:2013

Information Technology – Security Techniques – Vulnerability Handling Processes

This document gives guidelines on how to process and resolve potential vulnerability information in a product or online service.13 This was revised with a new version in 2019.

ISO/IEC 29147:2014

Information Technology – Security Techniques – Vulnerability Disclosure This document gives guidelines on the disclosure of potential vulnerabilities in products and online services. It details the methods a vendor should use to address issues related to vulnerability disclosure.15 This was revised with a new version in 2018.

ANSI/AAMI/ISO 14971: 2007/(R)2010

This document specifies a process for a manufacturer to identify the hazards associated with medical devices, including in vitro diagnostic (IVD) medical devices, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls.12 This was revised in 2019.

European Union (EU)

Medical Device Regulation (MDR) and In Vitro Diagnostic Medical Devices Regulation (IVDR)

Both MDR and IVDR Annex 1 discuss the same general safety and performance requirements.2,3 This section can be divided into two important parts:

1. **Performance and Safety.**

    a. Devices shall achieve the performance intended by their manufacturer and shall be designed and manufactured in such a way that, during normal conditions of use, they are suitable for their intended purpose.

    b. The characteristics and performance of the device should not be adversely affected during its lifetime under normal conditions of use.

  c. Devices must be designed, manufactured, and packaged to maintain their characteristics and performance during transport and storage.
  d. If the device is intended for use in combination with other devices or equipment the whole combination, including the connection system shall be safe and shall not impair the specified performance of the devices.2,3
  e. Correct and relevant information is provided in the labeling of the device to ensure its safe and correct use.

2. **Establish, implement, document and maintain a risk management system**
   a. Risk management plan
   b. Identification of known and foreseeable hazards.
   c. Risk evaluation and assessment
   d. Risk elimination or control
   e. Risk impact evaluation
   f. Reassess risk control measures[2,3]

MDCG 2019-16 Guidance on Cybersecurity of Medical Devices

Medical Device Coordination Group (MDCG) document provides the manufacturers with guidance on how to fulfill all the relevant essential requirements of Annex I to the MDR and IVDR concerning cybersecurity.[7]

The following provisions of the document are:

Premarket Activities:

1. Secure Design
2. Risk Management
3. Establish risk control measures
4. Validation, verification, risk assessment and benefit risk analysis
5. Technical documentation
6. Conformity assessment
7. Establish post-market surveillance system and plan

8. Post-market surveillance plan
9. Clinical evaluation process[7]

Post Market Activities

1. Risk Management
2. Modify risk control measures/corrective actions and patches
3. Validation, verification, risk assessment and benefit risk analysis
4. Maintain and update post-market surveillance system and plan
5. Trend reporting
6. Analysis of serious incidents
7. Post-market surveillance report
8. Periodic safety update report
9. Update technical documentation
10. Inform the Electronic system on vigilance[7]

Cybersecurity Resilience Act

The Cyber Resilience Act entered into force on 10 December 2024. The main obligations introduced by the Act will apply from 11 December 2027. The act aims to safeguard consumers and businesses buying software or hardware products with a digital component. A product with digital elements' means a software or hardware product and its remote data processing solutions, including software or hardware components, are being placed on the market separately.[19]

The Cyber Resilience Act addresses the inadequate level of cybersecurity in many products, and the lack of timely security updates for products and software.[8]

The Act is a comprehensive guide on products with digital elements, responsibilities of manufacturers and other economic operators who are placing their products in the EU. Same detailed provisions like other guidance in the EU, are secured design, risk management, sufficient and complete documentation, proper and adequate labeling including the CE marking indicating compliance, conformity assessment and vulnerability handling. A noteworthy provision of the Act is the requirement for manufacturers of products with digital elements to submit a Software Bill of Materials.8 There is also separate guidance on the Act on products with AI systems.

Related EU Laws and Guidelines

Network and Information Security (NIS) directive

General Data Protection Regulation (GDPR)[7]

This directive provides legal measures to boost the overall level of cybersecurity in the EU. The General Data Protection Regulation ('GDPR') regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU.[7]

European Health Data Space (EHDS) Regulation

The EHDS Regulation aims to establish a common framework for the use and exchange of electronic health data across the EU. It enhances individuals' access to and control over their personal electronic health data, while also enabling certain data to be reused for public interest, policy support, and scientific research purposes. This regulation enters into force last March 26, 2025.9

International Medical Device Regulators Forum (IMDRF)

Principles and Practices for Medical Device Cybersecurity[18]

The purpose of this IMDRF guidance document is to provide general principles and best practices to facilitate international regulatory convergence on medical device cybersecurity.[18]

General Principles

1. Global Harmonization

Convergence of global healthcare cybersecurity efforts is necessary to ensure that patient safety is maintained while encouraging innovation and allowing timely patient access to safe and effective medical devices. All stakeholders are encouraged to harmonize their approaches to cybersecurity across the entire life cycle of the medical device.18

2. Total Product Life Cycle (TPLC)

To effectively manage the dynamic nature of cybersecurity risk, risk management should be applied throughout the total product life cycle where cybersecurity risk is evaluated and mitigated in the various phases of the TPLC.18

3. Shared Responsibility

Medical device cybersecurity is a shared responsibility between stakeholders including the manufacturer, healthcare provider, users, regulator, and vulnerability finder.18

4. Information Sharing

The availability of timely information provides all responsible parties with enhanced capability to identify threats, assess risks, and respond accordingly. All stakeholders are encouraged to actively participate in Information Sharing Analysis Organizations (ISAOs).[18]

Premarket Considerations

1. Secured Architecture Design
2. Risk Management Principles for the TPLC
3. Security Testing
4. TPLC Cybersecurity Management Plan
5. Labeling and Customer Security Documentation
6. Documentation for Regulatory Submission[18]

Post-Market Considerations

1. Operating Devices in the Intended Use Environment
2. Information Sharing
3. Coordinated Vulnerability Disclosure
4. Vulnerability Remediation
5. Incident response[18]

Comparative Analysis of Cybersecurity Requirements of FDA, EU and IMDRF

The FDA, IMDRF, and EU regulatory frameworks operate on separate methodologies for medical device cybersecurity management within their respective legal frameworks yet they share common strategies when evaluated comparatively. All three regulatory frameworks require manufacturers to implement a risk-based approach to analyze cybersecurity risks and take mitigation steps during every stage of a medical device's lifecycle. All frameworks adopt the principle of Security by Design which requires security considerations to be integrated during the initial stages of product design and development. The continual emphasis remains on identifying and addressing vulnerabilities through threat modeling activities alongside security testing and vulnerability management program implementation. All three frameworks acknowledge the critical importance of post-market surveillance and prompt security patch deployment to counter emerging threats.

The use of Software Bill of Materials, creating an inventory of software components with its complete and detailed information, is present in the US FDA and IMDRF. While MDCG, EU MDR and IVDR do not explicitly mandate the SBOM unlike in the upcoming Cybersecurity Resilience Act, they still emphasize managing software components as part of risk management.

Despite these fundamental similarities, there are also key differences in their approaches and specific demands. The FDA provides detailed guidance documents, including premarket and post-market recommendations and has introduced legally binding requirements through Section 524B of the FD&C Act. The IMDRF strives to advance worldwide harmonization with established principles and best practices while emphasizing shared stakeholder responsibility throughout the total product lifecycle. The IMDRF offers a more internationally focused perspective without direct enforcement power. The EU MDR and IVDR stand out by explicitly including cybersecurity as a safety requirement within Annex I, making it legally enforceable. The EU framework also interacts with other EU regulations like the NIS Directive and GDPR. The EU has set a number of regulations and laws, making them a requirement. There are also potential differences in the level of prescriptive detail in specific requirements and the enforcement mechanisms. For instance, the FDA has the authority to refuse to accept submissions lacking cybersecurity information, while the EU relies on notified bodies for conformity assessment.

Healthcare Industry as Part of the Cybersecurity Infrastructure

Once a medical device is installed in a hospital, healthcare start-ups must implement cybersecurity measures and programs to secure the device and the sensitive data it carries during operation within the medical institution. As part of these requirements, it's crucial to train and educate end users and other stakeholders on medical device cybersecurity. The hospital industry also plays a vital role in securing medical devices and protecting patient data and privacy, often having its own set of cybersecurity standards and protocols that they implement when accepting a medical device from a healthcare start-up.

Outline Guide for Healthcare Startups

To help healthcare start-ups navigate the diverse cybersecurity standards and requirements from the US FDA, EU MDR, IMDRF, and others, the acronym "CYBERSECURED" has been developed as a comprehensive guide:

C – Control. Establish controls for the supply chain, components, and third-party services. Implement Software Bill of Materials.

Y – Yield to regulatory compliance. Ensure strict compliance with FDA and other regulatory cybersecurity mandates.

B – Best practices in cybersecurity. Adopt best practices in device design and development.

E – Encrypt and Authentication. Establish security controls to restrict unauthorized access.

R – Risk Management. Implement comprehensive risk management across the device lifecycle to ensure patient safety and device functionality.

S – Secured Architecture Design. Secure the device throughout its entire product lifecycle, starting from design and development.

E – Evaluation and Testing. Continuous and regular testing and validation of hardware, software updates against threats and vulnerabilities.

C – Continuous Monitoring. Continuously monitor and detect emerging threats, anomalies, and unusual behavior

U – Update. Update hardware and software regularly to meet emerging cybersecurity threats and vulnerabilities.

R – Response and Recovery Plans. Establish incident response and recovery plans for rapid mitigation and recovery.

E – Educate. Educate all relevant parties (employees, users, stakeholders) on medical device cybersecurity standards and protocols.

D – Documentation. Ensure thorough documentation and disclosure for regulatory and operational purposes (recording, monitoring, audit, compliance).

II. Conclusion

While there are different approaches to the matter of cybersecurity when looking into the different guidance and regulatory documents set by various agencies around the world, it is evident that there is a lot of common ground that they agree upon when it comes to securing medical devices.

The responsibility of a secured medical device not only lies with the regulatory agencies and the healthcare start-ups, the responsibility lies with all the stakeholders including the users, hospital management and third-party service providers. Only one mistake or a loophole in the system makes it vulnerable to threats or attacks. Everyone is responsible for the security and privacy of patient data.

It is of utmost importance for healthcare start-ups to adhere to the best standards of cybersecurity, be compliant with current regulations and continuously adapt to a fastchanging and evolving cybersecurity landscape to ensure secure and safe medical devices. It's fundamental for patient safety, device reliability, and lasting market viability.

It is crucial in building trust with users, healthcare providers, and regulatory agencies, fostering innovation and growth in this evolving field of healthcare industry.

REFERENCES

[1] AAMI TIR57:2016/(R)2023, Principles and practices for the cleaning and sterilization of reusable medical devices in health care facilities. AAMI. Accessed April 16, 2025. https://www.aami.org/detail-pages/product/aami-tir572016-r-2023-pdf-a152e000006j60wqaq

[2] Annex I - General safety and performance requirements. TUV SUD. Accessed April 18, 2025. https://de-mdr-ivdr.tuvsud.com/Annex-I-General-safety-andperformance-requirements.html

[3] Annex I - General safety and performance requirements - IVDR. TUV SUD. Accessed April 18, 2025. https://de-mdr-ivdr.tuvsud.com/Annex-I-General-safetyand-performance-requirements-IVDR.html

[4] ANSI/ISA-62443-4-1-2018, Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements. ISA. Accessed April 16, 2025. https://www.isa.org/products/ansi-isa-62443-4-1-2018-securityfor-industrial-au

[5] 5. Cybersecurity. FDA. Accessed April 15, 2025. https://www.fda.gov/medicaldevices/digital-health-center-excellence/cybersecurity

[6] 6. Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions. FDA. Accessed April 15, 2025. https://www.fda.gov/regulatory-information/search-fda-guidancedocuments/cybersecurity-medical-devices-quality-system-considerations-andcontent-premarket-submission

[7] 7. Cybersecurity of medical devices. European Commission. Accessed April 18, 2025. https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity._en.pdf

[8] 8. Cyber resilience act. European Commission. Accessed April 19, 2025. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[9] 9. European health data space regulation (EHDS). European Commission. Accessed April 20, 2025. https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en#what-is-the-ehdsregulation-about

[10] Framework for Improving Critical Infrastructure Cybersecurity. NIST. Accessed April 16, 2025. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[11] Health Insurance Portability and Accountability Act of 1996. CDC. Accessed April 17, 2025. https://www.cdc.gov/phlp/php/resources/health-insurance-portabilityand-accountability-act-of-1996-hipaa.html

[12] ISO/IEC 27001:2013, Information security management systems —Requirements. ISO. Accessed April 17, 2025. https://www.iso.org/standard/38193.html

[13] ISO/TS 22317:2015, Security and resilience — Business continuity management systems — Guidelines for business impact analysis (BIA). ISO. Accessed April 17, 2025. https://www.iso.org/standard/69725.html

[14] ISO 13485:2016, Medical devices — Quality management systems —Requirements for regulatory purposes. ISO. Accessed April 16, 2025. https://www.iso.org/standard/72704.html

[15] ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements. ISO. Accessed April 17, 2025. https://www.iso.org/standard/45170.html

[16] ISO 56002:2019, Innovation management — Innovation management system —Guidance. ISO. Accessed April 16, 2025. https://www.iso.org/standard/76097.html

[17] Postmarket Management of Cybersecurity in Medical Devices. FDA. Accessed April 16, 2025. https://www.fda.gov/regulatory-information/search-fda-guidancedocuments/postmarket-management-cybersecurity-medical-devices

[18] Principles and Practices for Medical Device Cybersecurity. IMDRF. Accessed April 18, 2025. https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech200318-pp-mdc-n60.pdf

[19] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 20 May 2024 on the European Health Data Space and amending Regulation (EU) 2016/679. EUR-Lex. Accessed April 19, 2025. https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=OJ:L_202401689

AUTHOR'S PROFILE

Ferdinan Tuazon holds a Master's degree in Medical Product Development Management (MPDM) at San José State University in San José, California. Before this, he earned a Bachelor's in Mechanical Engineering in the Philippines and worked for various companies as a field service engineer for medical equipment throughout the Philippines. He enjoys watching documentaries and science fiction.