TIC Council Position on Cybersecurity of Medical Devices in Europe

10 February 2022

Introduction

The increasing number of connected medical devices and ongoing digitisation in healthcare brings new market opportunities for the manufacturer and, more importantly, improvements in patient care. At the same time, it presents new and different types of risks to the security, safety, and privacy of medical devices. These connected medical devices range from sensor-based technologies such as wearables to implantable medical devices, such as pacemakers. To ensure the safe and secure use of connected medical devices, state-of-the-art technical as well as regulatory frameworks are necessary.

Coherent, consistent, and harmonised regulatory requirements are key to a high level of cyber-security and competitiveness at the European and international levels. Currently, however, an increasing amount of national cybersecurity requirements are published, which leads to an increased fragmentation of the European market[1].

The medical device regulation (MDR) that came into force on 26 May 2021 specifies that presumptive compliance to the general safety and performance requirements (GSPR) are preferably shown by conformity to harmonised standards. While such standards are currently under development this however means that no standard is harmonised under the MDR. As a matter of fact, the medical industry lacks any cyber-security related standards[2]. The MDCG guidance document on medical device cybersecurity (MDCG 2019-16) is a step in the right direction but which could be considerably improved to provide clear guidance on how to achieve appropriate levels of security. The lack of harmonised standards and clear guidance on cybersecurity creates confusion for manufacturers, which in turn hampers innovation in digital healthcare. Furthermore, even if the MDR provides for the use of technical specifications in the absence of harmonised standards, it is advantageous in terms of global trade if international standards are available as harmonised standards and not just technical specifications that have effect only on the European market.

TIC sector's recommendations to European policymakers

1. **Ensure the harmonised adoption of standards.** If guidance and/or regulatory requirements are not backed by harmonised standards, it leads to inconsistency in the evaluation process which subsequently undermines regulatory requirements. IEC 60601-4-5 for product assessment and IEC 81001-5-1 for

[1] Please see Annex I for a non-exhaustive mapping of medical device cybersecurity frameworks in key markets.
[2] In early 2021 the IEC TR 60601-4-5 was published. However, this is a technical report and not a standard.

secure development process requirements are examples of such standards that can provide valuable guidance. Additional standards are in the process of being developed and could be considered.

2. **Harmonise the approach to risk assessment.** STRIDE is an example of a threat modelling solution which can be incorporated without change into the Failure Mode and Effects Analysis (FMEA) which many medical manufacturers are already using. There needs to be a harmonised list of approaches to risk assessment, otherwise making it very difficult for a Notified Body (NB) to assess the risks in a consistent way. Additional guidance is provided by ISO/TR 24971:2020 Medical devices — Guidance on the application of ISO 14971, Annex F Guidance on risks related to security.[3]

3. **Harmonise high level test requirement**, developing requirements based on currently existing solutions such as Manimed, the CSA Cybersecurity Labelling Scheme, the Open Web Application Security Project, NIST, ENISA or MITRE. If there is no harmonised way of accessing criteria based on product category, risk category, functionalities and technologies, tests conducted would vary significantly, thus undermining the requirement of the whole framework.

4. **Ensure laboratory competency by requiring that cybersecurity assessments (consisting of tests and processes evaluations) be conducted by accredited laboratories[4] for medium and high-risk product categories according to MDR/IVDR**. Products having tests conducted by accredited laboratories would provide a higher level of assurance for the industry in addition to the above requirement of harmonisation of test categories based on risk.

5. **Support post-market activities** by utilizing existing database for vulnerability management data that enables vulnerability management, security management, and compliance (such as MITRE CVE database[5]). The database would be useful to ensure vulnerability management and risk mitigation processes are followed by manufacturers and implemented effectively. The database could be used to identify product names and versions, security flaws, misconfigurations, and impact measurements.

TIC sector's contribution to cybersecurity of medical devices

Risks to safety, security, and privacy exist at all levels of development of connected medical devices, requiring action throughout the product life cycle to protect patients. The independent third-party testing, inspection and certification industry has been assessing connected devices across multiple industries over the past

[3] ISO/TR 24971:2020(en): https://www.iso.org/obp/ui/fr/#iso:std:iso:tr:24971:ed-2:v1:en
[4] Accreditation is based on ISO/IEC 17025: Testing and Calibration Laboratories: https://www.iso.org/ISO-IEC-17025-testing-and-calibration-laboratories.html
[5] https://cve.mitre.org/

years, and has the necessary experience, capabilities, and trust to help ensure the safe and secure use of a connected medical devices.

Contact person: Martin Michelot, Executive Director Europe region, TIC Council, mmichelot@tic-council.org

TIC Council is the global trade federation representing the independent third-party Testing, Inspection and Certification (TIC) industry which brings together more than 90-member companies and organizations from around the world to speak with one voice. Its members provide services across a wide range of sectors: consumer products, medical devices, petroleum, mining and metals, food, and agriculture among others. Through provision of these services, TIC Council members assure that not only regulatory requirements are met, but also that reliability, economic value, and sustainability are enhanced. TIC Council's members are present in more than 160 countries and employ more than 300,000 people across the globe.

The Value of TIC Report

To learn more about TIC Council and its member's activities, the landmark report on the Value of the TIC sector, developed jointly by the international law firm Steptoe and the London-based consultancy Europe Economics is now available to read. This report illustrates, by using data and case studies, how the TIC sector benefits a variety of stakeholders and industries around the world. You can find the study here, and we welcome you to share it with anyone who might be interested.

ANNEX I

Mapping of the current Cybersecurity framework

National guidance for medical device cyber-security has steadily developed over the past few years. The following chapter is a non-exhaustive list of the current regulatory framework for medical devices in some key markets around the world.

IMDRF Principles and Practices for Medical Device Cybersecurity

The International Medical Device Regulators Forum (IMDRF) was founded in 2011 and is a forum for regulators around the world, with the aim to accelerate international medical device regulatory harmonisation. The documents created by IMDRF are used as guidelines for the development of local regulations and guidance documents. In terms of cybersecurity, the IMDRF published a guidance document entitled "Principles and Practices for Medical Device Cybersecurity" in 2020. The aim of the document is to provide concrete recommendations for all responsible stakeholders in connection with cyber security of medical devices (including In-Vitro Diagnostic devices). The guidance document explains the general principles and practices for medical device cyber security. The documents highlight the relevance of total product life cycle (TPLC) approach and introduces several key principles for each of the stages within the product life cycle. The guidance covers aspects from the pre- and post-market phase. The premarket requirements, such as secure by design, security risk management and security testing, are focused on manufacturers, while the post-market requirements are targeting all stakeholders, including operators. This approach highlights the understanding of the IMDRF on "shared responsibility" with all stakeholders, for ensuring high level of cyber security for medical devices. In addition to that, the document highlights the importance of harmonisation on international level.

European Union - MDCG 2019-16

The Medical Device Coordination Group (MDCG) is composed of representatives of all member states and provides advice to the Commission and assists the Commission and the Member States in ensuring a harmonised implementation of medical devices Regulations. The MDCG has published in December 2019 a guidance document on cyber security in medical devices (including In-Vitro diagnostic devices). The primary purpose of the document is to provide manufacturers with guidance on how to fulfil the relevant essential requirements found in Annex I of the respective regulations in terms of cybersecurity. The guidance is based on IMDRF principles and Practices for Medical Device Cybersecurity. It covers a broad range of requirements applicable to all stakeholders in the medical device supply chain from the manufacturer to the end-user. Compared to the FDA document the MDCG guidance covers both premarket and post-market requirements in one document.

The key component of the guidance is a security risk management process throughout the whole life cycle of the medical device and a secure by design approach. The guidance expands on various concepts of IT security, in particular the concept of confidentiality, integrity and availability (CIA), information security and operations security. However, the guidance also emphasizes the requirement for *appropriate* security, as security and safety are sometimes contradictory requirements in medical devices. They highlight the responsibility of the various parties involved in, integration of systems or devices, and of the operators of such devices, and the need to continuously review security measures to ensure that appropriate cybersecurity measures are in place and effective. The MDCG dedicates a whole chapter to documentation requirements. This also includes, beside the instructions for use and IT requirements, a reference to a Software Bill of Materials (SBOM). The post market requirement is supposed to be part of the post-market surveillance system.

Given that the medical device supply chain is complex and comprised of different stakeholders, the guidance document explains the applicability of other regulations and frameworks regarding cyber security of medical devices:

- NIS Directive: Provides framework to increase the general level of cyber security in the European Union

- GDPR (General Data Protection regulation): regulates the processing of personal data related to individuals in the European Union

- Cybersecurity Act: Provides a framework for the certification of cyber security products, services, and processes

United States - FDA

In 2013 the Food and Drug Administration (FDA) established the Cyber Security Working Group to keep up with quickly evolving technological developments in connected medical devices. Manufacturers of medical devices must address their device's cybersecurity risks as part of an FDA submission for marketing authorization. The FDA has published guidance and policy documents aimed at clarifying its expectations for manufacturers of connected medical devices.

In 2014 and 2016 the first two guidance documents from the FDA were published considering the premarket and post-marked requirements. The premarket guidance document will be replaced by a revision of the current version, with the first draft being published in 2018. The guidance explains several principles such as *security risk management,* including requirements on expected documentation. The new version of the guidance significantly increases the required cyber security design documentation for premarket submissions. The post-market guidance emphasizes a risk-based approach for the response to a new cyber security threat, after the device is placed on the market. The guidance leverages the requirements of NIST cyber security framework, such as *detecting* and *responding* to threats including *recovery* from an attack.

The FDA collaborates with other organizations on national and international level. In 2018 the FDA announced a collaboration with the U.S. Department of Homeland Security to implement a new framework for greater coordination in addressing cybersecurity risks in medical devices. Together with MITRE Cooperation, the FDA has developed a rubric that provides guidance for how an analyst can utilize the Common Vulnerability Scoring System (CVSS) as part of a risk assessment for a medical device.

Health Canada

To address cyber security in medical devices, Health Canada has published a cyber security guidance document "Pre-market Requirements for Medical Device Cybersecurity" in 2019. The guidance aims to improve device cyber security by mandating that manufacturers identify and analyse hazards associated with their devices, and to set controls and monitor their effectiveness. For the Canadian regulators, the primary responsibility for the safety and security of a medical device falls to the manufacturer. The manufacturers are requested to implement a security risk management process for any device that consists of software. The guidance applies to all classes of medical devices and core elements are secure by design, device specific security risk management, verification and testing and ongoing monitoring and response to new risk including disclosures of vulnerabilities and information sharing. The guidance emphasizes the adoption of NIST cyber security framework for establishing a security risk management process. The guidance further details the concept of cybersecurity by design and cybersecurity bill of materials for all third party and open-source software components.

France ANSM'S guideline - Cybersecurity of medical devices integrating software during their life cycle

The French authority for medical devices released a draft guidance document on cybersecurity for medical devices to enhance the existing European framework for medical devices (MDR) in 2019. The aim of the guidance is to minimize the risk of cyber-attacks on medical devices integrating software, throughout a total product lifecycle approach. The guidance requires manufacturers to undertake risk management, using both IT and medical device risk management methodology, and then align these approaches as part of manufacturers' implementation of quality management systems. The guidance addresses a total product life cycle (TPLC) approach by separating the recommendations into five phases of software lifecycle, in particular, design, development, first use, monitoring and end of life. The document refers to the French General Security Framework, which implements the principles of availability, integrity and confidentiality as baseline objectives. In addition to that the guidance specifies the requirements on the medical device manufacturers on auditability.

German Federal Office for Information Security - Cybersecurity Requirements for Network-Connected Medical Devices

In 2018, the German Federal Office for Information Security (BSI) published a recommendation for manufacturers on cyber security requirements for network-compatible medical devices. The aim of the document is to address security issues with connected medical devices considering device design and product development life cycle. It refers to the adoption of several best practices for cyber security and provide detailed measures to reduce a cyber security risk to an acceptable level. A central item of the recommendation is a security risk management process. Security bug fixes and patches to prevent the death or serious deterioration of health of a patient are corrective measures that must be reported in accordance with the Medizinprodukte-Sicherheitsplanverordnung (MPSV). Similar to the FDAs, Maude database the Federal Institute for Drugs and Medical Devices (BfArM) has a website on cyber security of medical devices, which lists potential corrective measures taken by manufacturers.