2021 IEEE/ACM 3rd International Workshop on Software Engineering for Healthcare (SEH) | 978-1-6654-4458-3/20/$31.00 ©2021 IEEE | DOI: 10.1109/SEH52539.2021.00011

On Medical Device Cybersecurity Compliance in EU

Tuomas Granlund
Solita Oy & University of Tampere
Tampere, Finland
tuomas.granlund@solita.fi

Juha Vedenpää
Solita Oy
Tampere, Finland
juha.vedenpaa@solita.fi

Vlad Stirbu
CompliancePal
Tampere, Finland
vlad.stirbu@compliancepal.eu

Tommi Mikkonen
University of Helsinki
Helsinki, Finland
tommi.mikkonen@helsinki.fi

***Abstract*—The medical device products at the European Union market must be safe and effective. To ensure this, medical device manufacturers must comply to the new regulatory requirements brought by the Medical Device Regulation (MDR) and the In Vitro Diagnostic Medical Device Regulation (IVDR). In general, the new regulations increase regulatory requirements and oversight, especially for medical software, and this is also true for requirements related to cybersecurity, which are now explicitly addressed in the legislation. The significant legislation changes currently underway, combined with increased cybersecurity requirements, create unique challenges for manufacturers to comply with the regulatory framework. In this paper, we review the new cybersecurity requirements in the light of currently available guidance documents, and pinpoint four core concepts around which cybersecurity compliance can be built. We argue that these core concepts form a foundations for cybersecurity compliance in the European Union regulatory framework.**

***Index Terms*—Medical device, regulatory requirements, cybersecurity, regulatory compliance**

I. Introduction

Regulatory compliance is one of the most important quality characteristics of a medical device – placing such device on the European Union (EU) market requires that the device complies with the EU regulatory framework. Also, the processes by which the device is being manufactured and maintained must be compliant with the regulations. In addition to medical device regulations, the manufacturer may need to comply with some other specific European legislation, depending on the product type.

At present, the EU medical device legislation is in transition, where three former directives will be replaced by two new regulations. A shared understanding of the contents amongst the practitioners is continuously being refined. This takes place in many ways, including new harmonized standards and guidance documents. In general, the transition is resulting in an increase in requirements, and a vital example of this is the more stringent requirements for cybersecurity. Furthermore, cybersecurity is a topical issue due to the acceleration of the digital transformation in health care and the increasing complexity of the new devices.

In this paper, we address the new cybersecurity requirements from a high viewpoint and propose an approach that can be used to build an understanding of the most fundamental aspects of cybersecurity compliance. It is crucial to fully understand the new requirements to implement them efficiently. This requires in-depth knowledge of practical methods and tools.

The rest of this paper is structured as follows. In Section II, we provide the legal background for the paper. In Section III, we address some apparent common challenges related to cybersecurity compliance concerning the new regulatory requirements. In Section IV, which forms the paper's core, we present our proposal for *Foundations of Medical Device Cybersecurity Compliance*. In Section V, we present a call for action for both regulatory authorities and medical device manufacturers. Finally, the concluding remarks are provided in Section VI.

II. Background

Currently, the EU medical device legislation is undergoing a significant change. Three former directives will be replaced by two new regulations: the Medical Device Regulation (MDR) 2017/745 [1] and the In Vitro Diagnostic Medical Device Regulation (IVDR) 2017/746 [2]. To address certain identified shortcomings of the former legislation, the new regulations emphasize the importance of clinical evaluation, risk management, post-market surveillance activities, and risk-benefit analysis throughout the product lifecycle [3]. In addition, particular new concepts are introduced, including now explicitly addressed requirements related to cybersecurity.

The increased cybersecurity requirements in the MDR and the IVDR affect mainly physical medical device products containing software and software that are the device itself. Also, specific requirements connected to the device's operational environment are presented, for example, requirements related to IT network characteristics.

In addition to MDR and IVDR, both of which are legally binding legislative acts and must be applied in their entirety, the EU Commission has mechanisms to provide more detailed technical specifications, in the form of harmonized standards and a range of non-binding guideline documents, for instance. The standards can be used to address General Safety and Performance Requirements (Annex I of MDR or IVDR), and guidance documents are intended to support the uniform application of the regulations within the EU.

Related to cybersecurity requirements, currently, the most important source for information is MDCG guidance document *MDCG 2019-16, Guidance on Cybersecurity for medical*

978-1-6654-4458-3/20/$31.00 ©2021 IEEE
DOI 10.1109/SEH52539.2021.00011

Authorized licensed use limited to: University of Durham. Downloaded on November 30,2024 at 22:00:14 UTC from IEEE Xplore. Restrictions apply.

devices [4]. At present, there are no harmonized standards against MDR or IVDR, which creates uncertainty for manufacturer concerning the appropriate set of standards to be selected to provide a 'presumption of conformity' against the regulatory requirements. However, the EU commissions recent draft standardization request [5] could be used to get an insight into the expectations of regulatory authorities related to applicable standards. The draft request includes a forthcoming standard *IEC 80001-5-1* [6], which is closely related to cybersecurity and relevant for the manufacturers. In addition to the sources mentioned above, the guidance documents *AAMI TIR57:2016 Principles for medical device security—Risk management* [7] and *IMDRF Principles and Practices for Medical Device Cybersecurity* [8] have been used as a reference in this paper.

III. Common challenges for the manufacturers

Based on the industry experiences, even the former regulatory requirements create certain challenges for the manufacturers [9]. While safety risks emerging from the cybersecurity dimension should be appropriately managed already today, some companies seem to have shortcomings in their security culture and processes [10]. Therefore, the gap between the new requirements and the existing implementation can be more significant than the actual difference between the existing and the new legislation is.

The EU regulatory framework is characterized by a certain level of complexity, which is true for cybersecurity requirements as well: the requirements in the new regulations concern many interconnected processes, and as a result, they are divided into different sections of the document. Therefore, the initial challenge for compliance is identifying and understanding all applicable provisions of the regulations. Furthermore, manufacturers have challenges addressing cybersecurity aspects within their risk management processes and implementing security actions into their design and development processes. It is evident that manufacturers need resources with in-depth knowledge about cybersecurity to deal with the new threats arising from accelerating digital transformation.

IV. Towards Medical Device Cybersecurity Compliance

In this section, we propose a high-level approach to address the new legislation's cybersecurity requirements. Special attention has been paid to the efficiency, making use of existing process requirements related to medical device design and development.

A. Risk relationship between safety and security

Medical device manufacturers are required to manage the risks related to their products throughout the devices' whole life cycle [1], [2], [8]. In practice, medical software risk management activities are implemented according to the requirements of *ISO 14971* [11] and *IEC 62304* [12]. In ISO 14971, the definition of risk is tightly bound to the concept of "physical injury or damage to the health of people, or damage to property or the environment." The risk management approach derived from this definition is characterized by the fact that its perspective focuses solely on safety-related risks, i.e., risks that affect the safety of the patients or the users. However, it is evident that the new regulations require a broader view of risk to address the new cybersecurity requirements.

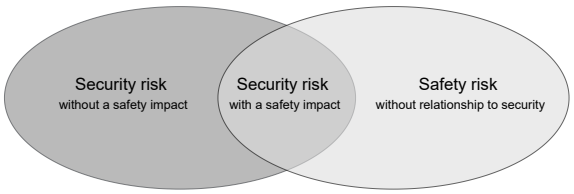

Fig. 1. Risk relationship between safety and security. Adapted from MDCG 2019-16, Guidance on Cybersecurity for medical devices.

The relationship between different risk classes is well documented [4], [7], [10] [13] (Figure 1). In the context of cybersecurity, there are three main types of risks:

- Security risk without a safety impact,
- Security risk with a safety impact,
- Safety risk without relation to security.

MDCG 2019-16 further elaborates the concept of "the relationship between cybersecurity risk management and patient safety management" by providing a table of examples in Annex II, from which more detailed risk types can be gathered. According to MDCG 2019-16, there can also be security risk controls with safety impacts and security risks with indirect safety impacts (e.g., risks related to device availability). When considering software-only devices, the safety risks are indirect by nature (i.e., incorrect or delayed diagnosis or treatment) [14], whereas physical devices can directly hurt the patient.

B. Aligned safety and security risk management processes

A safety risk management process can be considered as one of the core processes of medical device manufacturing [3]. Therefore, it is essential that the risk management process is working efficiently. When cybersecurity aspects are also considered, an aligned and efficient risk management process can be built utilizing the above-defined safety-security risk relationship as the baseline.

A security risk management process can be presented as a companion process to the safety risk management process (Figure 2), similarly to the usability engineering process in *IEC 62366-1* [7], [15]. Although not explicitly required [4], a separate security risk management process is recommended due to a broader perception of risk and to ensure complete and consistent security management [7] – the two processes differ in accordance to the nature of the risks that they control [10]. The security risk management process is used to manage those security risks that do not contain direct or in-direct safety impacts as they need to be managed to fulfill the cybersecurity requirements in MDR and IVDR. However, if a security risk has a safety impact, it will be propagated as an input item to safety risk evaluation as required by ISO 14971. Furthermore,

Authorized licensed use limited to: University of Durham. Downloaded on November 30,2024 at 22:00:14 UTC from IEEE Xplore. Restrictions apply.

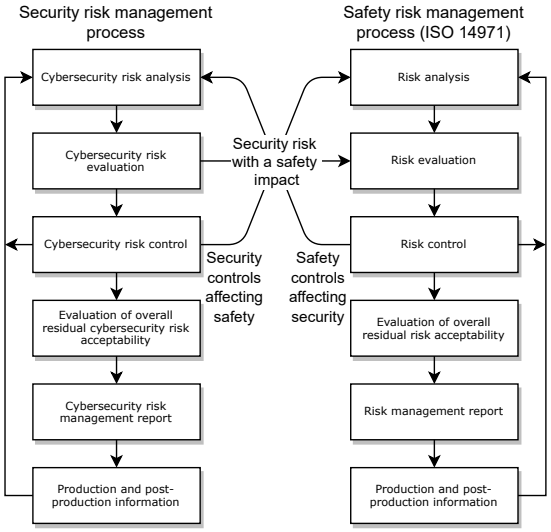

Fig. 2. Aligned safety and security risk management processes. Adapted from MDCG 2019-16, Guidance on Cybersecurity for medical devices and AAMI TIR57:2016, Principles for medical device security–Risk management.

as new risk control measures may introduce new risks, the impact of control must be analyzed from both safety and security perspectives.

MDCG 2019-16 has recognized potential challenges related to security risk controls – both too weak and too restrictive security controls may lead to undesired safety impact [4]. As a result, it is essential to ensure that the separate processes are well-aligned to enable the iteration of the device design between the processes through their logical connection points discussed above. Transparency is needed to set the balance between safety and security correctly and to address potential trade-offs explicitly.

C. Secure design and development lifecycle

As discussed above, security risk management is an integral part of the secure development lifecycle. One of the first steps of secure development is to perform threat modeling to identify potential security threats towards the device in its operating environment [4], [6]. In-depth security expertise is needed to capture all relevant security aspects fully - similarly as clinical expertise is needed in safety risk identification. Software security requirements are derived from the threat model to be implemented as appropriate risk controls.

Similarly to risk management being implemented in accordance to ISO 14971, medical software manufacturers generally have their product development processes implemented in compliance to the requirements of ISO 13485 and IEC 62304. From this point of view, it is recommended to extend the existing development processes with cybersecurity activities. This approach is supported by the forthcoming standard IEC 80001-5-1 [6]. Furthermore, the next version of IEC 62304 will likely also include specific cybersecurity provisions [16], [17].

TABLE I
CORRESPONDENCE BETWEEN MDCG 2019-16 DEFENCE-IN-DEPTH PRACTICES AND IEC 80001-5-1 PROCESSES.

MDCG 2019-16	IEC 80001-5-1
1. Security management	4.1 Quality Management 5.1 Software Development Planning
2. Specification of security requirements	5.2 Health Software Requirement Analysis
3. Secure by design	5.3 Software Architectural Design 5.4 Software Detailed Design
4. Secure implementation	5.1 Software Development Planning 5.5 Software Unit Implementation and Verification 5.8.3 File Integrity 5.8.4 Controls for private keys
5. Security verification and validation testing	5.5 Software Unit Implementation and Verification 5.6 Software Integration Testing 5.7 Software System Testing 5.8 Software Release
6. Management of security-related issues	4.1 Quality Management 5.1 Software Development Planning 6 Software Maintenance Process 7 Security Risk Management 8 Software Configuration Management Process 9 Software Problem Resolution Process 10 Quality Management System
7. Security update management	6.1 Security Update Management 6.2 Implementation Policy 6.3 Post-Market activities for Health Software
8. Security guidelines	5.8.2 Release documentation 6.3.1 Security update documentation 10.6 Accompanying Documents Review

MDCG 2019-16 approaches secure design and manufacturing process through "defense in depth" strategy. The strategy consists of the eight most necessary practices, which are no different from other cyber-physical systems [4]. The practices are presented in Table I. In addition, Table I shows how the practices can be mapped to IEC 80001-5-1 processes and requirements. As can be seen, the approaches taken by the documents are well-aligned, and IEC 80001-5-1 provides a more pragmatic view for implementing required security concepts. Therefore, IEC 80001-5-1 can be considered as a welcomed addition to the set of applicable medical device standards in the future.

D. Post-market cybersecurity activities

The new regulations require a more proactive approach to post-market surveillance from manufacturers. In general, the number of safety-related hazards of a medical device will stay relatively stable over time [4]. However, the same does not hold when considering cybersecurity threats, and, as a consequence, post-market cybersecurity activities need special consideration.

Authorized licensed use limited to: University of Durham. Downloaded on November 30,2024 at 22:00:14 UTC from IEEE Xplore. Restrictions apply.

Manufacturers are required to have post-market surveillance (PMS) system in place, which includes, depending on the class of the device, PMS reports, or Periodic Safety Update Reports (PSUR) [1], [2]. These reports should summarize the results and conclusions of the analysis of all the data from the market [4], including cybersecurity observations. Self-evidently, relevant changes in the security environment should be addressed as an input to the risk management process in a more timely manner. In addition, the vigilance process managing serious incidents and field safety corrective actions should be fine-tuned to consider also security aspects.

The key to efficient cybersecurity post-market surveillance process is identifying new security vulnerabilities proactively and resolving them timely yet without compromising safety or compliance. In addition to active vulnerability monitoring, manufacturers need a formal vulnerability disclosure process to communicate vulnerabilities with stakeholders and update technical documentation accordingly. In addition, the manufacturer must have a clear plan for recovery following cybersecurity incidents [8], also considering safe and secure decommissioning of the device.

V. Call for action

We believe that there is an urgent need for a call for action for regulatory authorities and medical device manufacturers. In the absence of harmonized standards against the MDR or IVDR, the crucial concept of 'presumption of conformity' is malfunctioning [3], creating unnecessary problems for the manufacturers. Combined with the complexity level of the regulatory framework and somewhat latent MDCG cybersecurity guidance, there is an evident shortcoming in the shared understanding of regulatory authorities' expectations related to cybersecurity requirements. We argue that IEC 80001-5-1 is an appropriate standard to address the cybersecurity regulatory requirements, and for this reason, its use should be adopted by the regulatory authorities and the manufacturers without undue delay.

In parallel, the manufacturers need to improve their underdeveloped culture of cybersecurity and set up their design and development processes according to the new requirements. Our proposed approach for the foundations of cybersecurity compliance serves as a good baseline for the implementation.

VI. Conclusions

Compliance with the regulatory requirements is one of the most important yet challenging aspects of medical device manufacturing. The new EU medical device legislation contains increased cybersecurity requirements, and the interconnection between the different documents, document sections, and requirements can be a challenge for the manufacturers. With regard to the current legislation transition and cybersecurity requirements, we identified the most essential sources for regulatory requirements and guidelines currently available.

With this paper, we proposed an approach that can be used to understand cybersecurity compliance and explain the key concepts. First, the foundations of medical device cybersecurity compliance are built on the risk relationship between safety and security. Second, an effective risk management approach can be derived from separate yet well-aligned safety and security risk management processes. Third, cybersecurity is implemented in practice within a well-controlled secure design and development process. Finally, medical devices' cybersecurity aspects must be considered throughout the whole lifecycle of the device.

Our research emphasized cross-analysis of the secure design and manufacture requirements of MDCG 2019-16 and IEC 80001-5-1. The practical outcome of this analysis is a table that shows the correspondence between the process requirements. Our results imply that forthcoming standard IEC 80001-5-1 provides an appropriate information source for manufacturers on how to implement the cybersecurity regulatory requirements in practice.

Acknowledgment. The authors would like to thank Business Finland and the members of AHMED (Agile and Holistic MEdical software Development) consortium for their contribution to preparing this paper.

References

[1] European Parliament and the Council. Regulation (EU) 2017/745 on medical devices, 2017.
[2] European Parliament and the Council. Regulation (EU) 2017/746 on in vitro diagnostic medical devices, 2017.
[3] Pitkänen, Heikki, Raunio, Leena, Santavaara, Ilona, and Ståhlberg, Tom. European Medical Device Regulations MDR & IVDR - A Guide to Market. Business Finland, 2020.
[4] Medical Device Coordination Group(MDCG). MDCG 2019-16 Guidance on Cybersecurity for medical devices, 2019.
[5] European Commission. Draft standardisation request as regards medical devices in support of regulation (EU) 2017/745 and in vitro diagnostic medical devices in support of regulation (EU) 2017/746, 2020. https://ec.europa.eu/docsroom/documents/43584. Accessed Dec 26 2020.
[6] IEC 80001-5-1 ED1, Committee draft, Sep 13 2019. Safety, security and effectiveness in the implementation and use of connected medical devices or connected health software. Part 5-1: Security - Activities in the product lifecycle.
[7] AAMI TIR57:2016. Principles for medical device security—Risk management, 2016.
[8] IMDRF Principles and Practices for Medical Device Cybersecurity. Draft document, Oct 1 2019. http://www.imdrf.org/docs/imdrf/final/consultations/imdrf-cons-ppmdc.pdf. Accessed Dec 26 2020.
[9] Williams, Patricia Ah, and Andrew J Woodward. "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem." Medical devices (Auckland, N.Z.) vol. 8 305-16. 20 Jul. 2015.
[10] ANSM'S guideline - Cybersecurity of medical devices integrating software during their life cycle (project), 2019.
[11] ISO 14971:2007. Medical devices – Application of risk management to medical devices, 2007.
[12] IEC/EN 62304:2006/A1:2015. Medical device software - Software lifecycle processes, 2015.
[13] IEC/TR 63069:2019. Industrial-process measurement, control and automation - Framework for functional safety and security, 2019.
[14] IMDRF "Software as a Medical Device": Possible Framework for Risk Categorization and Corresponding Considerations, 2014.
[15] IEC 62366-1:2015. Medical devices — Part 1: Application of usability engineering to medical devices, 2015.
[16] IEC 62304 ED2, Committee draft, Jun 10 2016. Health Software – Software Life Cycle Processes.
[17] Värri, Alpo, Kranz-Zuppan, Patty and de la Cruz, Richard. IEC 62304 Ed. 2: Software Life Cycle Standard for Health Software. In L. Ohno-Machado, & B. Séroussi (Eds.), Medinfo 2019: Proceedings of the 17th World Congress on Medical and Health Informatics (pp. 868-872), 2019.

Authorized licensed use limited to: University of Durham. Downloaded on November 30,2024 at 22:00:14 UTC from IEEE Xplore. Restrictions apply.