Medical Device Regulation and Cybersecurity: Achieving 'Secure by Design' for Regulatory Compliance

William S. Enns-Bray[1] and Kim Rochat[1]

[1] Medidee Services SA, Lausanne, Switzerland
{william.enns-bray,kim.rochat}@medidee.com

1 Introduction

The rapid evolution of information technology over the past 50 years is transforming our healthcare institutions from paper-based organizations into smart hospitals, a term now used by European Union Agency for Cybersecurity (ENISA) [1]. These changes are also associated with the systematic reliance on medical devices by both patients and healthcare providers. While these devices have the potential to advance personalized health solutions and improving the quality and efficacy of care, they nevertheless present significant security risks and challenges throughout the healthcare sector.

For example, hospitals are regularly targeted by ransomware, i.e. malware designed to block access to the victim's data, often by encrypting the data and then demanding a ransom to decrypt them. The ransomware Medjack infected hospitals worldwide between 2015 and 2017 and was estimated to have impacted over 6000 institutions. On May 17, 2017, WannaCry, another ransomware, affected more than 200'000 computers in over 100 countries, and triggered UK National Health Service (NHS) emergency plan designed to respond to major incidents. About 19'000 medical appointments were canceled as multiple trusts and primary care facilities were not able to operate normally.

More recently, COVID-19 has highlighted the benefit of remote consultations with doctors, even overcoming past resistance from some medical professionals. Yet malicious actors have been able to exploit the transition to remote communication during the pandemic through massive phishing campaigns designed to steal sensitive health data or potentially gain footholds for larger attacks.

Future medical devices will unlock new diagnostic and treatment capabilities, however adequate organizational and technological measures are needed to ensure safety and security are preserved. Thus, healthcare providers must dedicate sufficient resources to implement and maintain the appropriate security infrastructure for the evolving threat landscape. Meanwhile, manufacturers of medical devices must ensure they design and test their products according to state-of-the-art cybersecurity principles.

2 Cybersecurity Challenges for Medical Devices

In recent years, both European and American competent authorities have recorded increasing numbers of medical device recalls due to cybersecurity vulnerabilities. Examples of affected devices include telemetry servers where an attacker could silence or interfere with alarms [2], insulin pumps where an attacker could change the pump's

settings to either stop or over-deliver insulin to a patient [3], and implantable cardiac defibrillators where an attacker could access and manipulate an implantable device [4]. Commonalities between the different safety communications include the vulnerabilities associated with wireless communication, as well as the use of external security researchers to identify the cybersecurity vulnerabilities.

Historically, medical devices have exhibited high vulnerability to cybersecurity threats partly due to the low priority assigned to security requirements during development, as well as the slow maintenance cycles associated with highly controlled changes. Device manufacturers are often conservative when rolling out novel technologies which may have contributed to the slower rate of IT innovations in the healthcare sector compared to other industries. Cybersecurity expertise in healthcare is also often sorely lacking, resulting in medical devices falling further behind the state of the art in this domain. While this was not a critical issue in the decades preceding the internet, the rise of interconnectivity in the era of smartphones has significantly increased the use of medical devices and exacerbated the issues of what were already extremely soft targets.

ENISA defines the Internet of Things (IoT) as a "cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making," [5] suggesting medical devices are among the key drivers behind the growing IoT in the medical ecosystem. However, the design principles underpinning medical device development have traditionally focused on safety & effectiveness, which does not consider the security capabilities required for increased interconnectivity within larger network infrastructure or between medical devices themselves. In other words, manufactures have already been dedicating considerable resources to other domains of compliance within a heavily regulated industry, partly due to the lack of formal guidance or requirements on cybersecurity. As the regulatory landscape in Europe is changing, we expect that manufacturers will soon need to make security a greater priority in their devices.

3 Cybersecurity and Medical Device Regulation

3.1 EU Regulation 2017/745 (MDR)

Until recently, there has been a shortage of regulation and guidance on security requirements for medical devices marketed in Europe. However, the imminent application of the EU Medical Device Regulation (MDR) [6] will significantly increase the security expectations associated with making a medical device available on European markets. New safety and performance requirements explicitly state that software shall be developed and maintained in accordance with the state of the art, including information security. Thus, achieving compliance with the MDR clearly requires device manufacturers to demonstrate evidence of conformity with state of the art security principles.

3.2 Guidance on Cybersecurity for Medical Devices

Several organizations have already published guidance on cybersecurity for medical devices (e.g. FDA, IMDRF, AAMI, BSI). The present paper focuses on the cybersecurity guidance recently published by the medical device coordination group (MDCG),

an expert committee that advises the European Commission. This legally non-binding document [7] interprets the requirements of MDR and cites several well-known cybersecurity concepts, including how the CIA triad of confidentiality, integrity, availability relates to medical devices, processes, and data. The MDCG also expands the definition of 'risk' within the MDR to include security risks, while emphasizing the connection between security risk controls and new safety risks, and vice versa. This concept is linked to the balance between weak and restrictive security, where e.g. overly restrictive security controls could reduce availability of information which could manifest as a medical safety risk during operation. While the MDCG does not explicitly recommend a dedicated security risk management process, it is clear that all manufactures must consider security risk minimization as an implicit part of all regulatory requirements.

Joint responsibility between manufactures, operators, integrators, and end users is critical for securing medical devices. For manufacturers, the MDCG emphasizes the importance of establishing processes for secure installation and modification of software and communicating adequate security information to operators. Meanwhile for operators, responsibilities include adhering to security instructions and proactively contacting manufactures for additional information when necessary, e.g. using NEMA's well-known manufacturer disclosure statement (MDS2) [8]. Although this affirms the validity of using information as a security risk mitigation, information remains the weakest type of risk control (e.g. compared to design changes and protective features) and would likely be insufficient for claiming that a medical device is secure.

Concerning the secure design and manufacture of medical devices, the MCDG provides minimal technical or organizational details, apart from brief mention of the 'defense-in-depth strategy', which was likely derived directly from the IEC 62443 family of standards (more in on this in the next section). In summary, the MDCG links several modern security concepts to the MDR requirements, however the guidance alone is insufficient for implementing the technical state of the art.

3.3 State of the Art in Cybersecurity for Medical Devices

At the time of writing, there are no standards available recommending cybersecurity technical requirements specifically for medical devices. A new medical device standard, IEC TR 60601-4-5, is currently in development, but is not yet publicly available. Security of medical devices remains a present-day regulatory and safety issue, thus manufacturers are now faced with the double challenge of implementing state of the art security specifications, while staying prepared for future shifts in the landscape applicable standards. Fortunately, the solution to both challenges lies in the same family of standards: IEC 62443 Security for industrial automation and control systems (IACS).

For medical device manufacturers, achieving 'secure by design' requires both organizational and technological measures, which are addressed by IEC 62443-4-1 [9] and -4-2 [10], respectively. The first six security practices presented in IEC 62443-4-1 are already highly aligned with the well-established standard IEC 62304 (Table 1) for medical device software life cycle processes [11]. This does not imply that implementing IEC 62304 covers 75% of the requirements of IEC 62443-4-1, rather it suggests that specific processes should already be in place for supporting best security practices.

Concerning technical security requirements, IEC 62443-4-2 presents the concept of security capability levels (SLs) for product suppliers (i.e. legal manufacturers of medical devices), including which requirements can be allocated to system integrators and which requirements should be native to the device. This is aligned with the concept of joint responsibility published by MDCG, where the SLs could even be used by operators and their system integrators (e.g. in hospital & clinics) as explicit requirements in terms of security capabilities for the products they purchase (similar to the concept of MDS2). Moreover, manufacturers could translate the SLs achieved by their devices directly into device claims, which can be published in supporting information materials.

Table 1. Alignment between IEC 62443-4-1 and IEC 62304.

IEC 62443-4-1 Security Practice	IEC 62304 Life Cycle Process
Security management (Chap. 5)	Software development planning (Chap. 5.1) and software maintenance plan (Chap. 6.1)
Specification of security requirements (Chap. 6)	Software requirements analysis (Chap. 5.2)
Secure by design (Chap. 7)	Software architectural design (Chap. 5.3) and software detailed design (Chap. 5.4)
Secure implementation (Chap.8)	Software unit implementation and verification (Chap. 5.5)
Security verification and validation testing (Chap. 9)	Software unit implementation and verification (Chap. 5.5), Software integration and integration testing (Chap 5.6), and software system testing (Chap. 5.7)
Management of security related issues (Chap. 10)	Software problem resolution process (Chap. 9)

4 Proposed Method for Securing Medical Devices

Risk management (RM) and design control should be among the first processes implemented by medical device manufacturers. Early RM activities are critical for ensuring complete and comprehensive design inputs and verification & validation (V&V) activities. The fundamental processes within RM, i.e. risk analysis, risk evaluation, & risk control, do not change with respect to security risks. Instead, manufacturers must expand the dimensions of the risk analysis to identify security vulnerabilities and threats. The evaluation of security risks must also be augmented, e.g. by exchanging the concept of probability with a threat level, which can be expressed a function of exposure, detectability, as well as motivation, resources, and skill level of the attacker.

Despite the existence of effective RM tools, and the obligation of manufacturers to use them, unacceptable security risks remain widespread in present-day medical devices. The solution begins with device manufacturers increasing investment into the identification of security risks. A common approach uses threat modelling, an explicit

requirement of IEC 62443-4-1, where key characteristics (e.g. information flow, trust boundaries, attack vectors, etc.) must be identified, understood, reviewed, and updated by the development team. Early-phase threat modelling is also an ideal approach for injecting security into the design inputs, ensuring that the security control measures are properly verified. However, manufactures may need to bring in external expertise to ensure the identification, control, and verification measures are comprehensive enough.

Constructing effective testing methods and V&V plans requires a complete set of design inputs that have been carefully considered and regularly updated throughout product realization. Although security requirements are listed among the software specifications required by IEC 62304, no further details are provided since IEC 62304 is a 'process' standard and not a 'product' standard. IEC 62443-4-2 precisely addresses the gap left in medical device standards and guidance concerning technical security specifications. The security capabilities needed to attain a certain SL are divided into seven groups of foundational requirements (FRs), which also take into account the type of system (application, embedded device, host device, or network device).

For medical device manufacturers, the targeted SL for each FR will likely be SL 1 or SL 2 for many devices, depending on the outcome of threat modelling. Only in specific circumstances would a manufacturer consider intentional threats from adversarial attackers with sophisticated means, specific skills, and moderate to high resources and motivation (e.g. security risks with catastrophic impact on patient, user, or public safety). Once the necessary security capabilities have been translated from security risk control measures into software specifications, the verification activities under IEC 62304 take over, whereby the appropriate level of tests (i.e. code review and unit/integration/system tests) are implemented depending on the safety class of the associated software items. Adhering to this approach should establish clear traceability between any security risks, the applied control measures, and verification of their effectiveness.

5 Conclusion

Medical device manufacturers are late in the game concerning cybersecurity. While regulation and standards are catching up, what is currently needed from the industry is awareness, learning, and best practices. In this article, we have presented the framework of European regulation together with a methodology to achieve both regulatory compliance and devices that are secure by design. RM already forms the backbone of medical device development, therefore the methods proposed here should not be viewed as a fundamental change in processes, but rather as an expansion of existing RM tools and activities to include the identification and control of unacceptable security vulnerabilities. An effective RM process, which enables the identification and evaluation of security risks, will facilitate a wholistic understanding of those risks and their impact on the benefit-risk profile of the device. This approach will prepare medical device manufacturers for security-related questions from their notified bodies and ultimately provide patients and healthcare professionals with safer medical devices.

6 References

1. European Union Agency for Cybersecurity. Cybersecurity and resilience for Smart Hospitals. Published November 24, 2016. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals
2. Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers: Safety Communication. Published January 23, 2020. https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-certain-ge-healthcare-clinical-information-central-stations-and#vulnerabilities
3. Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks: FDA Safety Communication. Published June 27, 2019. https://www.fda.gov/medical-devices/safety-communications/certain-medtronic-minimed-insulin-pumps-have-potential-cybersecurity-risks-fda-safety-communication
4. Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication. Published March 21, 2019. https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home
5. European Union Agency for Cybersecurity. Defining and securing the Internet of Things: ENISA publishes a study on how to face cyber threats in critical information infrastructures. Published November 20, 2017. https://www.enisa.europa.eu/news/enisa-news/defining-and-securing-the-internet-of-things.
6. Regulation (EU) 2017/745 of the European parliament and of the council of 5 April 2017 on medical devices.
7. MDCG 2019-16 Guidance on Cybersecurity for medical devices. Published December 2019.
8. Manufacturer Disclosure Statement for Medical Device Security (MDS2). Publsuhed October 8, 2019. https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx
9. IEC 62443-4-1:2018 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements. Published January 15, 2018.
10. IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components. Published February 27, 2019.
11. IEC 62304:2006+AMD1:2015 CSV Medical device software – Software life cycle processes. Published June 26, 2015.