Developing a Compliant Cybersecurity Process for Medical Devices

Nadica Hrgarek Lechner
MED-EL Elektromedizinische Geräte GmbH
Fürstenweg 77a, 6020 Innsbruck, Austria
nadica.hrgarek@medel.com

Abstract. *Cybersecurity is growing in importance for medical device manufacturers, health care facilities, clinicians, patients, and regulators. The purpose of this paper is to propose the approach or methodology that can support medical device manufacturers to develop a compliant cybersecurity process as an integral part of their quality management systems to systematically manage cybersecurity risks.*

Keywords. cybersecurity, FDA, medical devices, privacy, quality management system, risk management, security, wireless

1 Introduction

Over the last few decades, medical devices have evolved from isolated equipment to networked devices with wireless communication and remote connectivity (Burns et al., 2016). In the past the focus was primarily on essential performance and safety, and less on security of medical devices. This paper provides some guidelines to develop a compliant cybersecurity process for design and development of medical devices. The paper is divided into four sections. Section 1 gives a brief overview of medical devices and emphasizes importance of cybersecurity for medical device manufacturers. The proposed cybersecurity model is briefly described in Section 2. In Section 3 we give some insights into cybersecurity as an integral part of a quality management system. Some conclusions are drawn in the last section.

Software was first used in medical devices in the 1980's (McHugh, 2015). According to Sarig (2012), the amount of software built into medical devices doubles about every two years. Embedding the software into medical devices can reduce development and maintenance costs. In addition, it can introduce new opportunities such as bringing new innovative products to the market faster, increasing clinical effectiveness, providing better services to end users through predictive and preventive maintenance, improving user experience, etc. As medical devices tend to change over time and become increasingly interconnected, implementation of new features including connections to the cloud, databases, third-party and open source software, IoT, hospital/health care facility networks, and other medical and non-medical devices leads to larger attack surfaces, associated with the increased complexity of the entire system and use models. To prevent cybersecurity incidents, Williams and Woodward (2015) point out that it is important to recognize the complexity of the operational environment as well as to catalog the technical vulnerabilities.

Software incorporated in connected medical devices such as remote-controlled drug infusion systems, defibrillators, cardiac pacemakers, and network-connected X-ray machines is vulnerable to cybersecurity threats. Medical devices that are connected to a public network like the Internet could be exploited by a threat actor through a single cybersecurity vulnerability. Some exploits could affect integrity of health data, availability of patient care, or even how a medical device operates. For example, malware infection can cause a device to slow down and miss critical interrupts and therefore, clinicians cannot trust the integrity of the sensor readings (Fu & Blum, 2013). Some vulnerabilities may cause the system to stop working which is especially dangerous for implantable, life-saving, and life-sustaining medical devices ("Bug can cause deadly failures when anesthesia device is connected to cell phones," 2014). Fu and Blum (2013) have raised some concerns about risks of depending on unsupported software (e.g., some medical devices still rely on Windows XP operating system with service packs and security patches). A compromised medical device may also serve as access point for entry into hospital networks to steal confidential data ("MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks," 2015). Using a networked medical device as means for intrusion may lead to compromise of other medical devices (e.g., in operating room), loss or exposure of sensitive and confidential patient information, or a safety issue. According to PwC's Health Research Institute (2017) consumer survey, 38% of consumers would be wary of using a hospital associated with a hacked medical device.

2 The Generic Cybersecurity Model for the Medical Device Industry

2.1 Background

Cybersecurity and information security are commonly used interchangeably; however, these terms differ. Cybersecurity is a part of information security (Spremić & Šimunic, 2018). Cybersecurity is defined as "the protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems" (ISACA, 2016, p. 9). The FDA (2014, p. 3) defines cybersecurity as "the process of preventing unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient". Information security "ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability)" (ISACA, 2016, p. 15).

The cybersecurity process plays a vital role in the field of medical and health technology. The main objective is to design and develop medical devices that are secure throughout the whole life cycle without compromising patient safety. As illustrated in Fig. 1, privacy and security must be considered early in conception and design of medical devices, become a part of medical device architecture, and end with obsolescence of medical devices.

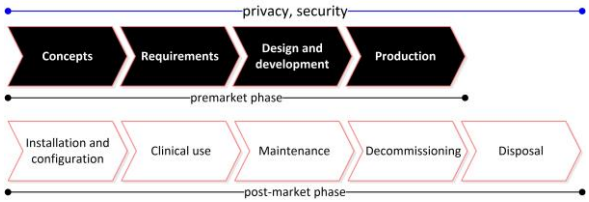

Figure 1. Medical device security life cycle

The model of confidentiality, integrity, and availability (also known as the CIA triad) is illustrated in Fig. 2. This model could be used as a starting point to implement a cybersecurity process. The main goal of the CIA triad is to apply appropriate security controls when data is stored, in processing, or in transit. The CIA triad alone is not enough to develop an effective cybersecurity strategy for medical devices. The ISO/IEC 27000 family of standards could assist the medical device manufacturers to keep key assets secure. Besides that, there are many federal government laws, regulations, standards, technical reports, and guidance combined with industry best practices that deal with information security and cybersecurity vulnerabilities of medical devices. As shown in Table 1, every component of the CIA triad can be mapped to applicable regulations, standards, and guidance documents. We suggest keeping a close eye on cybersecurity regulations and adapting processes accordingly to develop safe, effective, and secure medical devices. A brief overview of cybersecurity regulations and standards for medical devices is provided in (Hrgarek Lechner, 2017).

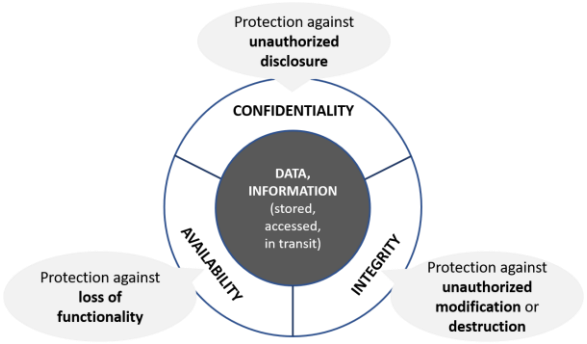

Figure 2. The CIA triad

Table 1. Mapping between CIA triad components and regulations, standards, and guidance documents

CIA triad component	Regulation, standard, guidance
Confidentiality	• AAMI TIR57 • BS EN 45502-1 • Content of Premarket Submissions for Management of Cybersecurity in Medical Devices • IEC TR 80001-2-8 • ISO/IEC 27000 • ISO/IEC 27001 • Medical Device Regulation • NIST cybersecurity framework • NIST SP 800-39 and 800-53 • Postmarket Management of Cybersecurity in Medical Devices • UL 2900-1 • UL 2900-2-1
Integrity	• AAMI TIR57 • BS EN 45502-1 • Content of Premarket Submissions for Management of Cybersecurity in Medical Devices • Health Insurance Portability and Accountability Act (HIPAA) • IEC 60601-1+AMD1 • IEC 62304+AMD1 • IEC 82304-1 • IEC TR 80001-2-8 • ISO/IEC 27000 • ISO/IEC 27001 • NIST cybersecurity framework • NIST SP 800-39 and 800-53 • Postmarket Management of Cybersecurity in Medical Devices • UL 2900-1 • UL 2900-2-1

CIA triad component	Regulation, standard, guidance
Availability	• AAMI TIR57 • BS EN 45502-1 • Content of Premarket Submissions for Management of Cybersecurity in Medical Devices • ISO/IEC 27000 • ISO/IEC 27001 • NIST cybersecurity framework • NIST SP 800-39 and 800-53 • Postmarket Management of Cybersecurity in Medical Devices

The FDA (2014) recommends considering five core functions of the NIST cybersecurity framework to guide cybersecurity activities. When developing a generic cybersecurity model that can be tailored to meet the regulatory requirements for the design and development of medical devices, we adapted the core functions of the NIST cybersecurity framework. The first version of the NIST framework ("Framework for Improving Critical Infrastructure Cybersecurity Version 1.0," 2014) was published in February 2014. According to a Gartner report ("Best Practices in Implementing the NIST Cybersecurity Framework," 2016), this version has been adopted by 30% of US companies and is expected to grow to 50% by 2020. In April 2018, a newer version of the NIST framework ("Framework for Improving Critical Infrastructure Cybersecurity Version 1.1," 2018) was released. The NIST's Framework Core consists of five functions: Identify, Protect, Detect, Respond, and Recover. Functions are subdivided into total 23 categories and 108 subcategories. Informative references are mapped to each subcategory.

2.2 Prerequisites

Our generic cybersecurity model that is further described in upcoming sections pre-assumes that the medical device manufacturer has established the risk management process to address and document all risks, including security risks with safety impact, throughout the whole medical device's life cycle. The elements of a cybersecurity vulnerability and management approach as part of the software validation and risk analysis are listed in FDA's (2014) guidance document. AAMI TIR 57 (2016), NIST SP 800-30 Rev. 1 (2012), HIMSS/NEMA Standard HN 1-2013 (2013), ISO/IEC 27005 (2018), OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation) approach (Alberts et al., 2003), and a white paper published by Medical Device Privacy Consortium (2014) can be used to guide the implementation of the security risk management process.

To determine appropriate security controls, the medical device manufacturer should start with identifying the critical assets that need to be protected, threats, and vulnerabilities that expose assets to the threats. As illustrated in Fig. 4, causal chain of security threats begins with a threat source initiating a threat event. If a threat source successfully exploits a device vulnerability and gains access to assets, this may result in an adverse impact due to a compromise of the device confidentiality, integrity, and/or availability.

Interfaces and threats can be identified using threat modeling (Domas & Merdinger, 2017). Threat modeling helps organizations to find security bugs early, understand security requirements, engineer and deliver better products, and address issues that other tools will not find (Shostack, 2014).

The CVSS calculator can be used to support vulnerability assessment ("Common Vulnerability Scoring System Version 3.0 Calculator," 2018). The calculator produces for each identified vulnerability a numerical score with a range between 0.0-10.0 reflecting its severity (i.e., none, low, medium, high, critical).

Following the initial risk identification phase, the manufacturer should perform security risk control activities for each identified risk and evaluate the overall residual security risk acceptability.

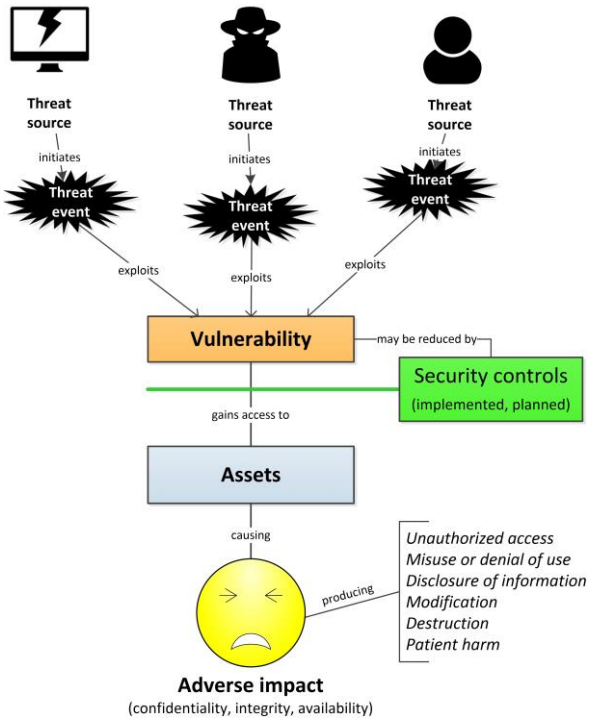

Figure 4. Illustrated causal chain of security threats Adapted from "Security risk analysis and management", by B. D. Jenkins, 1998, p. 4

2.3 Main Components

Our simplified cybersecurity model shown in Fig. 4 is based on the following three questions:

1. How to prevent cybersecurity incidents of medical devices in the first place?

2. How to detect cybersecurity vulnerabilities?
3. When a cybersecurity incident happens, how to respond to it?

The proposed model consists of the following three components: (1) prevention, (2) detection, and (3) incident response and recovery. Each component of the cybersecurity model has a corresponding set of security controls as further described in Section 2.4. Table 1 may be used to provide relevant informative references for the medical device industry.

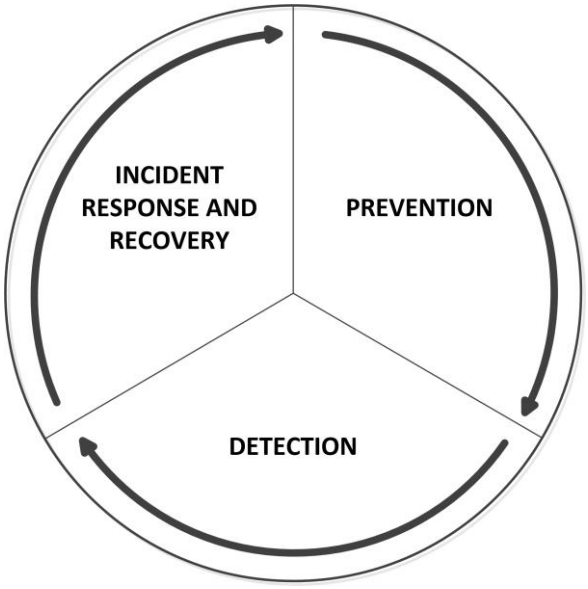

Figure 4. Generic cybersecurity model

Prevention is focused on designing medical devices from the start with cybersecurity in mind (i.e., security by design).

Detection means performing diverse types of security assessments to discover vulnerabilities that could be exploited and applying appropriate security controls to manage risks from cybersecurity threats that could impact the confidentiality, integrity, and/or availability of the medical device or the information processed by the device. It is important to note that cybersecurity needs to be assessed in the context of the larger system in which the medical device operates.

Incident response and recovery is needed to ensure that a medical device manufacturer has policies, procedures, and appropriate controls in place in case of a cybersecurity incident.

2.4 Security Controls

The FDA (2014) recommends developing a set of cybersecurity controls to assure medical device cybersecurity and to maintain medical device functionality and safety. The OWASP Secure Medical Device Deployment Standard (2017) can be used as comprehensive guide to the secure deployment of medical devices within a healthcare facility. This standard provides an overview of security controls that are divided into the following categories: purchasing controls, perimeter defences, network security controls, devices security controls, interface and central station security, security testing, and incident response.

Table 2 lists examples of security controls for each component of our cybersecurity model illustrated in Fig. 4. The table demonstrates that the highest number of security controls can be applied during prevention. More examples of security controls can be found in Annex E of AAMI TIR57 (2016).

Selection of appropriate security controls at various life cycle stages of a medical device depends on:

- Type of the medical device (e.g., device that contains software/firmware, device that contains programmable logic, software that is a medical device, mobile medical app, device that is considered part of an interoperable system, legacy device),
- Device classification,
- Intended use of the device,
- Operating environment in which the device is intended to be used,
- Intended users,
- User interaction with the device,
- Device's interaction with other devices on the network,
- Wired, remote, and wireless (e.g., Bluetooth, WiFi, wireless footswitch, Global System for Mobile Communications) interfaces,
- Communication protocols supported on internal and external interfaces,
- Technology (e.g., mobile, web, desktop, cloud computing, IoT),
- Used third-party components and open source software,
- External file inputs,
- Critical assets that need to be protected,
- Sensitivity levels of certain data (e.g., personally identifiable information, protected health information),
- Device's data flows,
- Data storage, etc.

Table 2. Examples of security controls

Component	Security control
Prevention	• Asset inventory • Code obfuscation • Conducting mock incidents • Cybersecurity policies and procedures • Data encryption technologies

Component	Security control
	• Data integrity controls (e.g., checksums, cryptographic checksums) • Database clusters • Default "deny" firewall policy • De-identification of patient data (e.g., anonymization, pseudonymization) • Established process to download and install security patches • Evaluation of cloud providers with respect to the security controls • Guidelines for secure development (e.g., avoiding exploitable code errors, validating data inputs before using or processing the data, storing local data securely, implementing access controls, etc.) • Instructions for the secure use of the device • Intrusion prevention systems • Malformed input (i.e., fuzz) testing • Network micro-segmentation • Operating system hardening • Partnerships with white-hat hackers and forensic experts to detect vulnerabilities that could be exploited • Physical locks on devices and their communication ports • Policies for classifying and categorizing all device data • Privileged user/account management (i.e., assigning roles using the principle of least privilege) • Publications describing how to avoid introducing common errors into the software that might become a vulnerability • Restricted software/firmware updates to authenticated code (e.g., code signing) • Sandboxing • Secure coding guidelines • Secure data transfer using encrypted connections (e.g., HTTPS, SSL, TLS, FTPS, etc.) • Security audits • Security awareness training for employees • Security code reviews • Security risk assessments • Self-descriptive user interface • Static binary and bytecode analysis • Static source code analysis • Threat intelligence • Threat modeling • User access controls (e.g., use of user ID and password, multi-factor authentication, account lockout after failed login attempts, automatic user logoff, changing default passwords at/prior to installation, password rules requiring use of strong passwords, lock screen function) • User authentication before permitting software/firmware updates • Version control systems • Vulnerability analysis
Detection	• Anti-virus software • Audit trails • Behavioral scanning • Endpoint protection tools (e.g., CrowdStrike Falcon®, Traps™) • Firewalls at the perimeter • Internal firewalls • Log monitoring • Malformed input (i.e., fuzz) testing • Malware testing • Network intrusion detection systems (e.g., Wireshark) • Port scanning tools (e.g., Nmap, Netcat) • Structured penetration testing • Vulnerability scanning tools (e.g., OpenVAS, Nexpose, Metasploit, Greenbone, Nessus) to scan for known vulnerabilities
Incident response and recovery	• Backup of device configuration • Cyber threat intelligence sharing via Information Sharing and Analysis Organizations (ISAOs) • Cybersecurity updates and patches • Data backup and restore • Established process to report detected cybersecurity incidents (e.g., coordinated vulnerability disclosure policy and practice) • Failsafe and recovery procedures • Incident response plan • Reverting to the previously installed version if the cybersecurity update fails

3 Integrating Cybersecurity into the Device Development Life Cycle

3.1 Challenges

The life cycle of medical devices involves design and development, design transfer, risk management, usability engineering, cybersecurity, clinical evaluation, servicing, decommissioning, disposal, and other processes. Cybersecurity shall be addressed throughout the whole lifecycle of a medical device.

According to a recent Deloitte's (2017) online poll, identifying and mitigating the risks of fielded and legacy connected devices presents the biggest challenge facing the medical device industry with respect to cybersecurity (30,1%). Additional challenges that connected medical devices presented to respondents included embedding vulnerability management into the design phase of medical devices (19,7%), monitoring and responding to cybersecurity incidents (19,5%), lack of collaboration on cyber threat management throughout connected medical device supply chain (17,9%), and meeting regulatory requirements (8,4%).

3.2 Integrating the Cybersecurity Process within a Quality Management System

According to the FDA guidance document (2016), cybersecurity shall be addressed in the following aspects of quality management systems: complaint handling, quality audit, corrective and preventive action, software validation and risk analysis, and servicing.

Integration of cybersecurity into the product development life cycle as part of a quality management system is not easy. The cybersecurity process spreads throughout the premarket and post-market phases of a medical device. The process is not isolated and the interfaces to the other processes within the organization and beyond it must therefore be identified and considered. Fig. 5 shows how the cybersecurity process is linked with other processes within a quality management system.

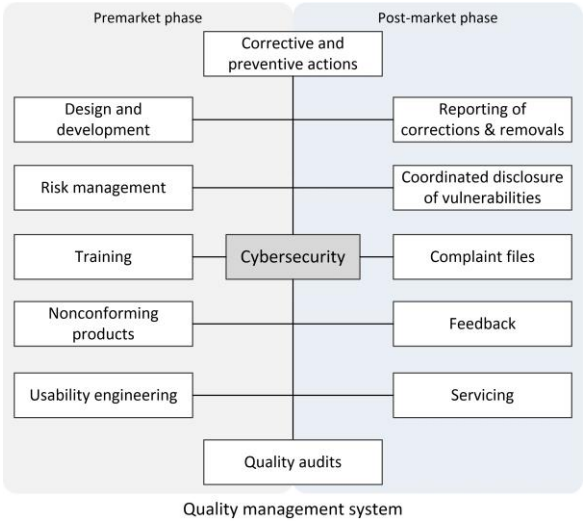

Figure 5. Position of the cybersecurity process within a quality management system

3.3 Implementation Considerations

Implementation of a cybersecurity program is a significant investment for any organization (Hrgarek Lechner, 2017). It requires support and endorsement from the top management to ensure availability of adequate resources and trained personnel for the cybersecurity process.

HITRUST ("Healthcare Sector Cybersecurity Implementation Guide," 2016) recommends the following seven steps to implement a cybersecurity framework in the healthcare sector: (1) prioritize and scope organizational components for framework adoption, (2) identify systems and existing risk management approaches within the scope, (3) create a desired risk management profile based on the organization's risk factors (Target Profile), (4) conduct a risk assessment, (5) create a current risk management profile based on assessment results (Current Profile), (6) develop a prioritized action plan of controls and mitigations (Action Plan), and (7) implement the Action Plan.

When developing a compliant cybersecurity process as an integral part of the quality management systems, the medical device manufacturers should consider the following:

- Gaining executive management support,
- Performing a gap analysis to identify discrepancies between the quality management system and the requirements set forth in the regulations and the organization's existing cybersecurity program (Hrgarek Lechner, 2017),
- Building an appropriate structure: e.g., a cross-functional cybersecurity team, a network of security champions ("Build a Network of Champions to Increase Security Awareness," 2017),
- Implementing an effective training and cybersecurity awareness program (Death, 2017),
- Working with external companies and security consultants providing security consulting services and performing penetration tests,
- Continuously monitoring regulatory requirements on medical device cybersecurity.

4 Conclusion

Historically seen, medical devices were designed and developed without design inputs related to cybersecurity. The next decade is likely to witness a considerable rise in cybersecurity threats of networked medical devices, wearable sensors, and other IoT devices. Since poor cybersecurity implementation may lead to data breach incidents and could have an adverse effect on patients, cybersecurity will play an increasingly significant role in operational safety and performance of medical devices. Cybersecurity also impacts business and top management support is needed to build a security culture within an organization.

Our generic cybersecurity model shows that an effective cybersecurity program is necessary at both

the premarket and post-market phases. Security must be built in from the start as part of the device development. A compliant cybersecurity process for medical devices requires addressing cybersecurity from design to obsolescence of medical devices being developed, marketed, and distributed. The selected security controls should mitigate cybersecurity risks early and prior to exploitation.

The cybersecurity process should be integrated into a quality management system considering the interfaces to the other processes within the organization and beyond it.

Disclaimer

The views and opinions expressed in this paper are those of the individual author and do not represent the approach, policy, or endorsement of the organization that is currently affiliated with the author.

Acknowledgments

The author would like to thank the anonymous reviewers for their valuable comments and suggestions which helped to improve the clarity and quality of this paper.

References

AAMI TIR57: Principles for medical device security—Risk management. (2016).

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). Introduction to the OCTAVE® Approach. Retrieved from https://resources.sei.cmu.edu/asset_files/UsersGuide/2003_012_001_51556.pdf

Best Practices in Implementing the NIST Cybersecurity Framework. (2016). Retrieved from https://www.gartner.com/doc/3188133/best-practices-implementing-nist-cybersecurity

BS EN 45502-1: Implants for surgery – Active implantable medical devices. Part 1: General requirements for safety, marking and for information to be provided by the manufacturer. (2015).

Bug can cause deadly failures when anesthesia device is connected to cell phones. (2014). Retrieved from https://arstechnica.com/information-technology/2014/04/bug-can-cause-deadly-failures-when-anesthesia-device-is-connected-to-cell-phones/

Build a Network of Champions to Increase Security Awareness. (2017). Retrieved from https://www.gartner.com/smarterwithgartner/build-a-network-of-champions-to-increase-security-awareness/

Burns, A. J., Johnson, M. E., & Honeyman, P. (2016). A Brief Chronology of Medical Device Security. *Communications of the ACM*, 59(10), 66–72. doi:10.1145/2890488

Common Vulnerability Scoring System Version 3.0 Calculator. (2018). Retrieved from https://www.first.org/cvss/calculator/3.0

Death, D. (2017). *Information Security Handbook. Develop a threat model and incident response strategy to build a strong information security framework*. Birmingham: Packt Publishing.

Deloitte. (2017). Medical devices and the Internet of Things: A three-layer defense against cyber threats. Retrieved from https://de.slideshare.net/DeloitteUS/medical-devices-and-the-internet-of-things-a-threelayer-defense-against-cyber-threats

Domas, S., & Merdinger, S. (2017). Designing Robust Medical Devices that Are Ready for Enterprise Security Scanning. *Biomedical Instrumentation & Technology: Cyber Vigilance: Keeping Healthcare Technology Safe and Secure in a Connected World*, 51(6), 26–29. doi:10.2345/0899-8205-51.s6.26

FDA. (2014). Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff. Retrieved from https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf

FDA. (2016). Postmarket Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff. Retrieved from https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

Framework for Improving Critical Infrastructure Cybersecurity Version 1.0. (2014). Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. (2018). Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Fu, K., & Blum, J. (2013). Controlling for Cybersecurity Risks of Medical Device Software. *Communications of the ACM*, 56(10), 35–37. doi:10.1145/2508701

Health Insurance Portability and Accountability Act of 1996. (1996).

Healthcare Sector Cybersecurity Implementation Guide. (2016). Retrieved from https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf

HIMSS/NEMA Standard HN 1-2013: Manufacturer Disclosure Statement for Medical Device Security. (2013).

Hrgarek Lechner, N. (2017). An Overview of Cybersecurity Regulations and Standards for Medical Device Software. In *Proceedings of the Central European Conference on Information and Intelligent Systems (CECIIS 2017)* (pp. 237–249). University of Zagreb, Faculty of Organization and Informatics Varaždin.

IEC 60601-1+AMD1: Medical electrical equipment – Part 1: General requirements for basic safety and essential performance. (2012).

IEC 62304+AMD1: Medical device software – Software life cycle processes. (2015).

IEC 82304-1: Health software – Part 1: General requirements for product safety. (2016).

IEC TR 80001-2-8: Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2. (2016).

ISACA. (2016). Cybersecurity Fundamentals Glossary. Retrieved from https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf

ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary. (2018).

ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements. (2013).

ISO/IEC 27005: Information technology – Security techniques – Information security risk management. (2018).

Jenkins, B. D. (1998). *Security risk analysis and management* [White paper]. Retrieved from https://www.nr.no/~abie/RA_by_Jenkins.pdf

McHugh, M. (2015). Medical Device Software and Technology: the past, present and future. *BEAI Spectrum*, Spring, 28–32.

Medical Device Privacy Consortium. (2014). Security Risk Assessment Framework for Medical Devices.

MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks. (2015). Retrieved from https://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html

NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments. (2012). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View. (2011). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations. (2013). Retrieved from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

OWASP. (2017). OWASP Secure Medical Device Deployment Standard Version 1.0. Retrieved from https://www.owasp.org/images/c/c3/SecureMedicalDeviceDeployment.pdf

PwC Health Research Institute. (2017). Top health industry issues of 2018: A year for resilience amid uncertainty. Retrieved from https://www.pwc.com/us/en/health-industries/assets/pwc-health-research-institute-top-health-industry-issues-of-2018-report.pdf

Sarig, I. (2012). Meet Embedded Software Quality Challenges in Medical Device Development. *MEDS Magazine*, Jan., 24–28.

Shostack, A. (2014). *Threat Modeling: Designing for Security*. Indianapolis: John Wiley & Sons.

Spremić, M., & Šimunic, A. (2018). Cyber Security Challenges in Digital Economy. *Proceedings of the World Congress on Engineering 2018 (WCE 2018) Vol I* (pp. 341–346). London.

UL 2900-1: UL Standard for Safety for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements. (2017).

UL 2900-2-1: UL Standard for Safety for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems. (2017).

Williams, P. A. H., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, 2015(8), 305–316. doi:10.2147/MDER.S50048