An Overview of Cybersecurity Regulations and Standards for Medical Device Software

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

Abstract*. This paper discusses current cybersecurity regulations and standards for medical device software set by government agencies and agencies developing industry and international standards such as the FDA (Food and Drug Administration), CFDA (China Food and Drug Administration), ISO (International Organization for Standardization), IEC (International Electrotechnical Commission), UL (Underwriters Laboratories), and others. The concepts described within this paper can be utilized by medical device manufacturers in order to establish a cybersecurity program as part of their quality management systems. In general, there are three complementary ways based on the NIST (National Institute of Standards and Technology) cybersecurity framework that can be used to remove gaps in the organization's cybersecurity. The first way focuses on designing software products that take cybersecurity into account (i.e., prevention). The second way is to perform security and penetration testing and to apply other cybersecurity controls to reduce attacks and vulnerabilities that could be exploited (i.e., detection). The third way emphasizes maintenance plan in case of a cyberattack (i.e., response and recovery).*

Keywords. cybersecurity, FDA, information security, medical device software, security risk management

1 Introduction

This paper is divided into five sections. The first section focuses on history and cybersecurity in the context of medical devices. Definitions of the key terms used in this paper are provided in the second section. The third section provides an overview of the cybersecurity regulations, standards, and guidelines for medical device software. The fourth section investigates how to incorporate cybersecurity into the quality management system. Some conclusions are drawn in the final section.

Cybersecurity is a complex, multidisciplinary computing-based discipline that has its roots in the 1960s. First paper on security and privacy in computer systems was published by Ware (1967). In 1970, Ware finalized a report about security controls for computer systems and emphasized that design of a secure system must provide protection against the various types of vulnerabilities such as accidental disclosure, deliberate penetration, active infiltration, and physical attack (Ware, 1970). Ware (1970) stated the following general characteristics as desirable in a secure system: flexible, responsive to changing operational characteristics, auditable, reliable, manageable, adaptable, dependable, and assuring configuration integrity.

Burns et al. (2016) identified four periods in the history of medical devices which evolved from the non-networked and isolated equipment to networked devices incorporating remote access, wireless technology, and complex software. The first period (1980s–present) involved concerns about the complex systems and accidental failures. The second period (2000–present) involved concerns about the security and reliability of implantable medical devices. The third period (2006–present) raised questions about the vulnerability of medical devices to unauthorized parties. In the fourth period (2012–present), attention has turned to the cybersecurity of medical devices. A recent KPMG's survey (2015) of 223 healthcare executives revealed many information security concerns: malware infecting systems, HIPAA (Health Insurance Portability and Accountability Act) violations/compromise of patient privacy, internal vulnerabilities related to employee theft/negligence, medical device security, and aging IT hardware. According to a recent study from the Ponemon Institute (2016), healthcare organizations experience, on average, a cyberattack almost monthly as well as the loss or exposure of sensitive and confidential patient information. Arxan's (2016) study on application security reveals that 90% of 126 mobile health and finance apps tested had at least two critical security vulnerabilities.

In January 2017, the U.S. Food and Drug Administration issued a safety communication confirming cybersecurity vulnerabilities found in St. Jude Medical's Merlin@home wireless transmitter that could affect the company's line of implantable cardiac devices ("Cybersecurity Vulnerabilities

Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication", 2017). Two months later, the FDA issued a warning letter to Abbot. The company failed to confirm that all required corrective and preventive actions were completed to correct and prevent recurrence of potential cybersecurity vulnerabilities associated with its Merlin@home device, originally manufactured by St. Jude Medical ("Abbott (St Jude Medical Inc.) 4/12/17", 2017). In August 2017, the FDA issued another safety communication confirming a firmware update that was needed as a corrective action to reduce the risk of patient harm due to potential exploitation of cybersecurity vulnerabilities for certain Abbott implantable cardiac pacemakers ("Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication", 2017).

2 Key Definitions

This section provides definitions of the key terms.

Asset is "a person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value" ("A Glossary of Common Cybersecurity Terminology", 2017).

Availability aims to keep information accessible when it is needed (Svensson, 2016).

Confidentiality aims to prevent sensitive information (e.g., medical records) from falling into the wrong hands (Svensson, 2016).

Cybersecurity is "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" (FDA, 2014, p. 3). "Cybersecurity ensures that appropriate safeguards are in place to reduce the risk of failure because of cyberattack, which could be initiated by the introduction of malware into the medical equipment or by unauthorized access to configuration settings in medical devices" (ANSI/AAMI CI:86, 2017, p. 30).

Data and systems security is defined as "operational state of a medical device in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability" (AAMI TIR57, 2016, p. 2).

Information security is "protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" (AAMI TIR57, 2016, p. 3). ISO/IEC 27000 (2016) defines information security as preservation of confidentiality, integrity, and availability of information.

Integrity seeks to prevent information from being altered by unauthorized users (Svensson, 2016).

Security is "protection of information and data so that unauthorized persons or systems cannot read or modify them and authorized persons or systems are not denied access to them" (ISO/IEC 12207, 2008, p. 7). The most common security objectives are as follows: data confidentiality, data integrity, access control, authentication, authorization, and non-repudiation.

Threat is "a circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society" ("A Glossary of Common Cybersecurity Terminology", 2017).

Vulnerability is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source" (AAMI TIR57, 2016, p. 5).

3 Cybersecurity Regulations and Standards for Medical Device Software

In this section we provide an overview of currently published cybersecurity regulations, standards, and guidelines in the context of medical device software. This overview can serve as an input to establish and maintain procedures that address cyberattack prevention, detection, and response/recovery.

3.1 FDA and CFDA Guidance Documents, ISO/IEC 29147, and ISO/IEC 30111

The FDA has issued three guidance documents on cybersecurity listed in Table 1. The FDA guidance documents (2014, 2016) are applicable to devices that contain software (including firmware) or programmable logic, and to software that is a medical device, including mobile medical applications.

Table 1. FDA guidance documents on cybersecurity

Title	Year issued
Guidance for Industry – Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software	2005
Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff	2014
Postmarket Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff	2016

According to the FDA guidance (2005), computer software changes to address cybersecurity vulnerabilities should be validated. The agency (FDA, 2005) also recommends developing a single cybersecurity maintenance plan.

When preparing FDA medical device premarket submissions, the manufacturers have to demonstrate an effective cybersecurity management. The FDA (2014) recommends establishing a cybersecurity vulnerability and management approach as part of the software validation and risk analysis. Such approach contains the following activities: 1) identify assets, threats, and vulnerabilities associated with medical devices, 2) assess the impact of threats and vulnerabilities on device functionality and end users/patients, 3) assess the likelihood of a threat and of a vulnerability being exploited, 4) determine risk levels and mitigations, and 5) assess residual risk and risk acceptance criteria (FDA, 2014). The FDA premarket submission documentation should include the following information related to the cybersecurity of the medical device: 1) hazard analysis, mitigations, and design considerations, including a specific list of all cybersecurity risks and cybersecurity controls for the device; 2) a traceability matrix that links the actual cybersecurity controls to the cybersecurity risks that were considered in the design of the device; 3) a plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device; 4) controls ensuring integrity (e.g., remain free of malware) of the medical device software from development to device delivery; 5) device instructions for use and product specifications related to recommended cybersecurity controls appropriate for the intended use environment (e.g., use of anti-virus software, how to configure a firewall) (FDA, 2014).

The FDA guidance (2016) on postmarket management of cybersecurity in medical devices recommends implementing a proactive, comprehensive cybersecurity risk management program. Such a program can be established as part of the risk management process and may include: monitoring cybersecurity information sources (e.g., CVE (Common Vulnerabilities and Exposures) standard for information security vulnerability names (https://cve.mitre.org)); robust software lifecycle processes; assessing and detecting presence and impact of vulnerabilities; definition of communication processes for vulnerability intake and handling; using threat modeling on a regular basis; adopting a vulnerability disclosure policy and practice; deployment of mitigations that address cybersecurity risk early and prior to exploitation (FDA, 2016). For example, the Common Vulnerability Scoring System (CVSS) version 3.0 (www.first.org/cvss) can be used for vulnerability assessment.

The FDA guidance documents (2014, 2016) recommend the use and adoption of the voluntary NIST cybersecurity framework's five core functions: Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). In January 2017, NIST issued a draft cybersecurity framework version 1.1. Table 2 provides the NIST framework core functions and corresponding cybersecurity outcomes.

Table 2. NIST cybersecurity framework core functions and outcome categories (NIST, 2017)

Function identifier	Outcome categories
ID	Asset management, business environment, governance, risk assessment, risk management strategy, supply chain risk management
PR	Access control, awareness and training, data security, information protection processes and procedures, maintenance, protective technology
DE	Anomalies and events, security continuous monitoring, detection processes
RS	Response planning, communications, analysis, mitigation, improvements
RC	Recovery planning, improvements, communications

The CFDA published the guidance on the technical reviews of the cybersecurity registration of Class II and III medical devices that connect to networks for the purpose of exchanging or storing data, or for remote control ("CFDA Spells Out Cybersecurity Requirements", 2017).

ISO/IEC 29147 (2014) and ISO/IEC 30111 (2013) standards are recognized by the FDA. ISO/IEC 29147 can be used as a guideline to address issues related to disclosure of potential vulnerabilities in products and online services. ISO/IEC 30111 gives guidelines how vendors should investigate, triage, and resolve potential vulnerabilities in products and online services.

3.2 BS EN 45502-1

BS EN 45502-1 (2015) defines the requirements that are generally applicable to Active Implantable Medical Devices (AIMD). There are also standards for particular AIMDs. For example, ANSI/AAMI CI:86 (2017) standard for cochlear implant systems requires security protection of wireless links and risk management, interoperability, and cybersecurity of the medical device.

Subclause 5.4 of BS EN 45502-1 standard requires adequate consideration of data security and protection from harm caused by unauthorized information tampering. "When communication with the implantable part of an ACTIVE IMPLANTABLE MEDICAL DEVICE through wireless communication channels is provided, the MANUFACTURER shall evaluate INFORMATION SECURITY through the RISK MANAGEMENT

PROCESS, and apply the appropriate RISK CONTROL measures to protect the patient from HARM. *Compliance is checked by the inspection of the RISK MANAGEMENT FILE*." (BS EN 45502-1, 2015, p. 13)

As part of medical device regulatory submissions, the manufacturers shall provide documented evidence that safety risks due to IT security threats which may compromise confidentiality, integrity, and availability of data have been adequately assessed and managed. The manufacturers shall also consider no detection, response, and recovery of IT security threats.

3.3 IEC 62304+AMD1, IEC 82304-1, and IEC 60601-1+AMD1

IEC 62304+AMD1 (2015) defines the requirements for medical device software life cycle processes. This standard requires including security requirements in the software requirements. For example: security requirements related to the compromise of sensitive information, authentication, authorization, communication integrity, audit trail, and system security/malware protection. Furthermore, when a problem is detected in the medical device software, a problem report shall be prepared. The standard requires including a statement of criticality with respect to effect on performance, safety, or security. The second edition of IEC 62304 is currently being drafted to align with IEC 82304-1. This edition will require a process for managing risks associated with data and system security, including privacy.

IEC 82304-1 (2016) provides requirements for the safety and security of health software products. According to this standard, potential sources of harm include breach of security and reduction of effectiveness. As part of general requirements definition and initial risk assessment, the manufacturers of the health software products can use the following sources of information on security vulnerabilities: publicly available reports from authorities, publications by suppliers of operating systems and third party software (IEC 82304-1, 2016). Table 3 lists requirements of IEC 82304-1 standard with respect to security. The requirements apply throughout the whole life cycle including design, maintenance, postmarket communication, decommission, and disposal of health software products.

Table 3. IEC 82304-1 (2016) requirements for health software products with respect to security

Clause	Requirement
4.1 b)	As part of general requirements definition and initial risk assessment, the manufacturer shall determine and document the characteristics related to the safety and/or security of the health software product and identification of hazards and estimation of the associated risk(s).
4.2 d)	When defining use requirements, the manufacturer shall determine and document privacy and security requirements addressing areas such as authorised use, person authentication, health data integrity and authenticity, and protection against malicious intent.
4.2 f) 3)	When defining use requirements, the manufacturer shall determine and document requirements to support timely security patches and updates.
4.5 f)	When defining system requirements, the manufacturer shall include the functionality for intended use and features that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use, as applicable.
4.5 g)	When defining system requirements, the manufacturer shall include the functionality for intended use and features that protect essential functions, even when the software security has been compromised, as applicable.
4.5 h)	When defining system requirements, the manufacturer shall include the functionality for intended use and methods for retention and recovery of product configuration by an authenticated privileged user, as applicable.
7.2.2.2 c)	The instructions for use shall contain any operational security options for the use of the health software.
7.2.2.3	The instructions for use shall list all warnings and notices for safety and/or security related to the use of the health software product and explain or expand them when they are not self-explanatory.
7.2.2.4 c)	The instructions for use shall contain operational security options for the health software to be set at installation time.
7.2.2.9	The instructions for use shall contain all information necessary for the user or the responsible organization to safely decommission and dispose of the health software. This shall include, where appropriate, safeguarding personal and health-related data in connection with security and privacy.
7.2.3.1 g)	The technical description shall provide all data that is essential for safe and secure operation, transport and storage, and measures or conditions necessary for installing the health software, and preparing it for use. This shall include any technical security options that can be configured within the health software

Clause	Requirement
	product, and that are available to the responsible organization. Such security may include: 1) configuration options (e.g., minimum list of network ports and computer services that are required), 2) software options (e.g., turn on encryption settings, change default login credentials), 3) operational options (e.g., auditing and logging management settings).
7.2.3.1 h)	The technical description shall include a description of what the software does when a failure to maintain security is detected. The description shall include any impact to patient care, data or clinical workflow.
7.2.3.1	The manufacturer shall provide instructions in the technical description for the user and/or the responsible organization on how to deal with changes of the hardware and software platforms (e.g., with patches/updates of antivirus/firewall software, system libraries, firmware, and others), and how to select appropriate platform settings to support the security goals and security capabilities.
7.2.3.2 b)	If the health software is intended to be used in an IT-network that is outside the control of the health software manufacturer, the manufacturer shall provide, as part of the technical description, instructions necessary for this use, including the technical specifications of the IT-network necessary for the health software to achieve its purpose, including security specifications and protection against malware or similar.
8.2	Where the manufacturer decides that software maintenance is relevant or necessary, for instance, due to detected errors that can have an impact on safety and/or security, the manufacturer shall develop the modification of the health software product in compliance with Clause 5 of IEC 82304-1.
8.4	The manufacturer shall inform users of the health software product and impacted responsible organizations about the security vulnerabilities the manufacturer has become aware of, and of changes in regulatory requirements that impact the use of the health software product.
8.4 c)	In the case of software maintenance, the manufacturer shall make information available to users and to the responsible organizations of the availability of the updated version of the health software product, and provide information about any impact on safety and/or security of the modified software, where appropriate.
8.5	The user or the responsible organization shall be able to safely decommission and dispose of the health software product at the end of its useful life, including, where appropriate, safeguarding personal and health-related data in connection with security and privacy.

IEC 60601-1+AMD1 (2012) is a product safety standard for manufacturers of medical electrical equipment and systems. As part of the risk management process for Programmable Electrical Medical Systems (PEMS), subclause 14.6.1 of the standard provides examples of possible causes for hazards associated with PEMS. These examples include consideration of lack of integrity of data, lack of data security, including its effects on data privacy, and particularly vulnerability to tampering, unintended interaction with other programs and viruses (IEC 60601-1+AMD1, 2012). If the PEMS is intended to be incorporated into an IT-network that is not validated by the PEMS manufacturer, subclause 14.13 d) requires from the manufacturer to make available instructions for implementing such connection including the technical specifications of the network connection of the PEMS including security specifications. Viruses, worms, unauthorized software updates, or upgrades can lead to hazardous situations associated with IT-networks (IEC 60601-1+AMD1, 2012).

3.4 AAMI TIR57, ISO 14971, and NIST SP 800-30 Revision 1

AAMI TIR57 (2016) supports medical device manufacturers by providing guidance on methods to perform information security risk management for a medical device. The main goal is to “manage risks from security threats that could impact the confidentiality, integrity, and/or availability of the device or the information processed by the device” (AAMI TIR57, 2016, p. vii). This technical information report follows the basic structure of ISO 14971 (2007) standard and recommends “the creation of a separate risk analysis process focused specifically on impacts that are identified by a security analysis” (AAMI TIR57, 2016, p. 5). It also incorporates some principles from NIST SP 800-30 Revision 1 (2012), a guideline for conducting risk assessments of federal information systems and organizations.

AAMI TIR57 (2016) distinguishes between security risks that include breach of data and systems security and reduction of effectiveness, security risks with potential safety impact, and safety related risks that are covered by ISO 14971 standard. “Security risk is based on an assessment of the likelihood that a threat will successfully exploit a device vulnerability, an event that could lead to an adverse impact due to a compromise of system confidentiality, integrity, and/or availability" (AAMI TIR57, 2016, p. x).

The security risk management process recommended by AAMI TIR57 (2016) consists of the following activities: 1) security risk management plan, 2) security risk analysis, 3) security risk evaluation, 4) security risk control, 5) evaluation of overall residual security risk acceptability, 6) security risk management report, and 7) production and post-production information.

To support the manufacturers to identify characteristics related to the security of their medical devices, Annex D of AAMI TIR57 (2016) provides a list of questions that cover the following areas: essential performance of the device, data storage of Personally Identifiable Information (PII)/private data assets and non-PII data assets, data transfer, authentication and authorization, logging and auditing, physical security, device/system updates, hardening, emergency access, malware/virus protection, backup/disaster recovery, and labeling (i.e., instructions for use with respect to security).

3.5 IEC 80001 Family

IEC 80001-1 (2010) defines the following key properties for medical IT-networks: safety, effectiveness, data and systems security.

IEC/TR 80001-2-2 (2012) provides a framework for the disclosure of security-related capabilities and risks necessary for managing the risk in connecting medical devices to IT-networks. This technical report assists the health delivery organizations, medical device manufacturers, and IT vendors in the application of risk management when creating or changing a medical IT-network.

IEC TR 80001-2-8 (2016) provides guidance to health delivery organizations and medical device manufacturers how to apply the framework outlined in IEC/TR 80001-2-2 (2012). This technical report identifies the following security controls: automatic logoff, audit controls, authorization, configuration of security features, cyber security product upgrades, health data de-identification, data backup and disaster recovery, emergency access, health data integrity and authenticity, malware detection/protection, node authentication, person authentication, physical locks on device, third-party components in product life cycle roadmaps, system and application hardening, security guides, health data storage confidentiality, transmission confidentiality and integrity.

IEC TR 80001-2-9 (2017) provides guidance to health delivery organizations and medical device manufacturers for identifying, developing, interpreting, updating, and maintaining security assurance cases for networked medical devices. It also provides guidance for the selection of appropriate security controls listed in IEC/TR 80001-2-2 (2012) to establish security capabilities.

3.6 Medical Device Regulation (MDR)

New European regulation on medical devices requires IT security, protection and confidentiality of personal data at various development stages (refer to Table 4).

Table 4. MDR requirements addressing security and data protection ("Official Journal of the European Union L 117", 2017)

Page	MDR requirement
101	Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.
107	The instructions for use shall contain for devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.
121	Minor software revisions shall require a new UDI-PI and not a new UDI-DI. Minor software revisions are generally associated with bug fixes, usability enhancements that are not for safety purposes, security patches or operating efficiency.
171	Description of the arrangements to comply with the applicable rules on the protection and confidentiality of personal data, in particular: • organisational and technical arrangements that will be implemented to avoid unauthorised access, disclosure, dissemination, alteration or loss of information and personal data processed; • a description of measures that will be implemented to ensure confidentiality of records and personal data of subjects; • a description of measures that will be implemented in case of a data security breach in order to mitigate the possible adverse effects.
264	For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.

3.7 UL 2900 Family

In 2016, the Underwriters Laboratories launched a Cybersecurity Assurance Program (CAP) that provides testable cybersecurity criteria for assessing software vulnerabilities, malware, and security controls in network-connectable products and systems. Here are some examples of network-connectable products and systems: medical devices and their accessories, medical device data systems, in vitro diagnostic devices, health IT, wellness devices, automotive, industrial control systems, smart home, fire systems, alarm systems, IoT (Internet of Things), etc.

Table 5 provides a list of UL's 2900 series of cybersecurity standards. UL 2900-1 (2017) specifies general product requirements for network-connectable products and systems, whereas UL 2900-2-1 and UL 2900-2-2 that were published in 2016 specify industry product requirements. New UL 2900-3 standard is currently under development and will specify general requirements for the organization and product development security life cycle processes for network-connectable products.

Table 5. UL 2900 cybersecurity standards

Identifier	Title
UL 2900-1	Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements
UL 2900-2-1	Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare Systems
UL 2900-2-2	Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems

EMERGO has recently published on its web site that a set of UL 2900 standards to address medical device cybersecurity issues will soon be adopted by the FDA ("UL 2900 Cybersecurity Standards Set for FDA Adoption", 2017).

3.8 ISO/IEC 27000 Family

The ISO/IEC 27000 family of standards helps organizations to protect their information assets such as financial information, intellectual property, employee details, etc.

ISO/IEC 27000 (2016) provides an overview and the vocabulary of Information Security Management Systems (ISMS).

ISO/IEC 27001 (2013) is an international security standard that provides the requirements for establishing, implementing, maintaining, and improving an ISMS. "The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed." (ISO/IEC 27001, 2013, p. v) ISO/IEC 27001 (2013) specifies total 114 security controls across the following areas: A.5 Security policy, A.6 Organization of information security, A.7 Asset management, A.8 Human resources security, A.9 Physical and environmental security, A.10 Communications and operations management, A.11 Access control, A.12 Information systems acquisition, development and maintenance, A.13 Information security incident management, A.14 Business continuity management, A.15 Compliance.

ISO/IEC 27032 (2012) provides guidelines for organizations to address common cybersecurity risks such as social engineering attacks, hacking, malware (short for malicious software), spyware, other potentially unwanted software. It also provides a framework for information sharing, coordination, and incident handling.

ISO 27799 (2016) provides guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

3.9 HIPAA

The Health Insurance Portability and Accountability Act of 1996 is a healthcare legislation in the United States that specifies requirements to safeguard the privacy and security of Protected Health Information (PHI). It was introduced in 1996 and become Public Law 104-191. The HIPAA legislation requires, among other things, that "e-mails to patients containing health-related information must be encrypted in transit, unless the patient has written authorization on file for the organization to send their information unencrypted" (Wittkop, 2016, p. 38). Failure to comply with HIPAA may result in civil and criminal penalties (Robichau, 2014).

The HIPAA Privacy Rule generally states that any paper/electronic PHI provided to employees of a healthcare organization must be appropriate to their job and in keeping with adopted internal policies (Robichau, 2014). This approach is called the minimum necessary standard. Subject to the HIPAA Privacy Rule are so-called covered entities. There are three types of covered entities: 1) insurance carriers or health plans (e.g., Medicare, Medicaid, Health Maintenance Organization (HMO), TRICARE, etc.), 2) health care clearinghouses that submit health care claims for a provider, and 3) any health care providers that transmit health information electronically in connection with transactions regulated by the US Department of Health and Human Resources. Each covered entity must appoint a HIPAA officer who is responsible for HIPAA compliance and all aspects of information privacy and security.

To ensure appropriate protection of electronic PHI, the HIPAA Security Rule outlines three different safeguards: 1) administrative (i.e., security management process, security personnel, information access management, workflow training and management, periodic evaluation of security policies and procedures), 2) physical (i.e., facility access and control, workstation and device security), and 3) technical (i.e., access control, audit controls, data integrity control, transmission security) ("Summary of the HIPAA Security Rule", 2013).

4 Integration of Cybersecurity into the Quality Management System

Implementation of a cybersecurity program is a significant investment for any organization. Such a program should be designed to protect computers, mobile platforms, medical devices, networks, software, medical records, proprietary, confidential or personal information, and other information assets from unintended or unauthorized access, use, theft, transmission, storage, modification, destruction, or denial of service.

Medical device manufacturers without cybersecurity programs could use the NIST cybersecurity framework as a reference to establish one. According to a Gartner report ("Best Practices in Implementing the NIST Cybersecurity Framework", 2016), the NIST cybersecurity framework that was published in February 2014 has been adopted by 30% of US companies and is expected to grow to 50% by 2020. Robert Ford, Abbott's Executive Vice President of Medical Devices, said that their cybersecurity program was built around the following key elements: 1) a dedicated product cybersecurity multifunctional group to ensure cybersecurity is part of the design process, 2) cybersecurity medical advisory board made up of leading health care professionals to advise, counsel, and partner with Abbott, and 3) a network of reputable and experienced third-party cybersecurity research companies to challenge and validate Abbott's systems ("Focus on Cybersecurity", 2017). Adopting a coordinated vulnerability disclosure policy is encouraged (FDA, 2016).

The FDA (2014) recommends developing a set of cybersecurity controls in order to assure medical device cybersecurity and to maintain medical device functionality and safety. To reduce vulnerabilities, four security experts ("Top 10 cybersecurity must-haves for 2017", 2017) recommended the following ten measures to protect patient data and keep it out of cybercriminals' hands: 1) risk assessments, 2) disaster recovery and contingency plans, 3) dedicated security operations team to handle security, hunt threats, educate staff on latest threats, and perform penetration tests, 4) business associate/vendor scrutiny, 5) better employee training, 6) layered defense, 7) improved tech hygiene, 8) cybersecurity partnerships, 9) better software, and 10) forensic consultants to provide insights on weaknesses, liabilities, and security reports.

Performing a periodical gap analysis can be a helpful method to evaluate the policies, standard operating procedures (SOPs), and processes implemented by the organization in order to identify discrepancies between the quality management system and the requirements set forth in the cybersecurity regulations, guidelines, best practice standards, and the organization's existing information security or cybersecurity program. After identifying the gaps, a cybersecurity improvement plan can be developed. The purpose of this plan is to provide management with insight into the areas within the quality management system which need to be improved.

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.

4.1 Complaint Handling

The complaint handling process should track customer security concerns and consider cybersecurity incidents as a cause for complaints.

4.2 Quality Audit

Quality audits are useful to examine implementation of the cybersecurity program to confirm compliance with regulatory requirements, policies, and SOPs.

4.3 Corrective and Preventive Action

The Corrective and Preventive Action (CAPA) sub-system should consider analysing processes, quality audit reports, returned products, service records, complaints, and other sources of quality data in order to identify cybersecurity vulnerabilities as a cause for non-conforming products, or other quality issues. The CAPA process should plan corrective and preventive actions in order to react on cybersecurity incidents.

4.4 Software Life Cycle Processes

Cybersecurity should be considered throughout the whole life cycle of the medical device software, including design inputs, security requirements, secure software architectural design, secure coding, maintenance plans, and updates.

According to the FDA (2016), robust software lifecycle processes include mechanisms for: monitoring third party software components for new vulnerabilities throughout the device's total product lifecycle, and design verification and validation for software updates and patches that are used to remediate vulnerabilities, including those related to OTS software. Similar to the usability engineering process, the manufacturers could establish a security engineering process.

Writing secure, robust code and performing code reviews with security in mind is an essential skill for every software engineer. The Microsoft Security Development Lifecycle (SDL) could be used as a guideline to help developers build secure software and to address security requirements ("Microsoft Security Development Lifecycle", 2017). Furthermore, software engineers can use threat modeling (Shostack, 2014), the OWASP (Open Web Application Security Project) Secure Coding Practices – Quick Reference Guide (2010), SAFECode (Software Assurance Forum for Excellence in Code) checklists, and training material ("Best Practices for Security & Privacy", 2016). Further information about secure systems engineering and how to integrate security activities into software engineering life cycle processes can be found in (Goertzel et al., 2007).

Using the OWASP's annual list of the top ten security risks during development and security testing of medical device software may help to adequately address and correct the most critical security flaws. OWASP identified the following top ten application security risks in 2017: injection flaws, broken authentication and session management, cross-site scripting (XSS), broken access control, security misconfiguration, sensitive data exposure, insufficient attack protection, Cross-Site Request Forgery (CSRF), using components with known vulnerabilities, and underprotected APIs ("OWASP Top 10 Application Security Risks – 2017", 2017). The following top ten mobile security risks in 2016 were identified by OWASP: improper platform usage, insecure data storage, insecure communication, insecure authentication, insecure cryptography, insecure authorization, client code quality, code tampering, reverse engineering, and extraneous functionality ("Mobile Top 10 2016-Top 10", 2017).

Medical devices with weak security that are connected to a public network (Internet) are more exposed to ransomware attacks. For example, in May 2017, the global ransomware attack has infected and encrypted some medical devices and computers at medical facilities ("Medical Devices Hit By Ransomware For The First Time In US Hospitals", 2017). A multi-layered security model can be implemented to prevent network-based and application-based attacks. For example, when users connect their laptops to public Wi-Fi networks, they are running the risk of exposure to malware or viruses that can later infect the corporate network. A firewall can stop attacks at the network perimeter, but it may not be able to stop an attack that comes from a trusted source ("Layered security is IT's best defense", 2016). Therefore, security at each layer must work together.

Security testers are responsible for performing security and penetration testing. "Security testing is a type of vulnerability assessment. The security tester takes on the role of a hacker and tries her best to break into the organization's IT environment. The purpose of such a test is to find any vulnerabilities within an organization's IT environment and how the vulnerabilities could be exploited in a real-world hacker attack." (Svensson, 2016, p. 2) Security testing includes methods such as penetration testing with man-in-the-middle attacks, fuzzing, scanning, and auditing the software (Knott, 2015).

4.5 Security Risk Management Process

The risk management process required by ISO 14971 should begin early in the development process and also address security risks. "To manage postmarket cybersecurity risks for medical devices, a company should have a structured and systematic approach to risk management and quality management systems consistent with 21 CFR part 820." (FDA, 2016, p. 14)

The security risk management process should address the following elements: 1) identification of assets, vulnerabilities, and threats, 2) security risk evaluation, 3) implementation of security risk control measures, 4) assessment of residual risk and risk acceptance criteria, and 5) submission of relevant information to appropriate stakeholders (e.g., users, regulators, health delivery organizations).

AAMI TIR57 (2016) recommends establishing a companion security risk management process in addition to the safety risk management process required by ISO 14971 (2007). According to AAMI TIR57 (2016), top management should provide adequate and qualified personnel to perform the security risk management process (i.e., personnel should be knowledgeable in evaluating security threats and vulnerabilities, and should have experience with hardware and software architecture, design, and security test methods). In addition, top management should review the suitability of the security risk management process at defined intervals (AAMI TIR57, 2016). There are three different approaches that can be used for security risk assessment: 1) threat-oriented, 2) asset/impact-oriented, and 3) vulnerability-oriented (AAMI TIR57, 2016). "A security risk management report summarizes the evaluation, assessment, mitigation activities, and traceability to the verification reports of security controls that ensure a device is reasonably secure.” (AAMI TIR57, 2016, p. 14) A security risk management file can be created and maintained as a separate document or integrated with the overall risk management file of the medical device (AAMI TIR57, 2016).

4.6 Resources and Training

Top management should provide qualified personnel and tools to perform tasks related to cybersecurity.

Many different types of security threats have developed over time: Trojan horses, worms, computer viruses, sniffers, rootkits, backdoors/trapdoors, key loggers, spyware, malware, ransomware, social engineering, reverse engineering (undesired access to intellectual property), code tempering (changes to application behaviour), botnets, insider attacks, etc. According to Meeuwisse (2017), complex digital environments in large organizations need a range of cybersecurity experts. He identified the following six main cybersecurity tasks and skills (i.e., functions) with corresponding roles: 1) management (e.g., Cyber Risk Manager, Chief Information Security Officer (CISO)/Chief Cybersecurity Officer, Cybersecurity Architect), 2) cyber audit and assessment (e.g., Audit Manager, Auditor, etc.), 3) event monitoring and alerts (reactive operations) (e.g., Security Incident and Events Manager, Cybersecurity and Network Intrusion Analysts, etc.), 4) proactive operations (e.g., Access Administrators, Security Risk Consultants, Cybersecurity Analysts, etc.), 5) environment testing (e.g., Attack and Penetration Testers (Ethical Hackers), Vulnerability Assessors), and 6) specialists (e.g., Security Controls Designer, External Security Specialist, Digital Forensics Specialist, Cryptologist, Cryptanalyst, Anti-Malware/Anti-Virus Specialist, Software Security Specialist). Meeuwisse (2017) recommends having a CISO or Chief Cybersecurity Officer role on the main executive board of an organization to ensure that the organization has appropriate security processes, policies, practices, and procedures in place.

In December 2013, the Government in the UK held 4 workshops with 51 individuals from large businesses, small and medium-sized enterprises, and universities. The Government found that businesses looked for a wide range of professional cybersecurity qualifications and accreditations as displayed in Fig. 1 (HM Government, 2014). In addition to cybersecurity experts, companies like Bigfoot Biomedical, Inc. hire security hackers (“Security Hackers Help Bigfoot Biomedical Keep Patient Info Secure”, 2017).

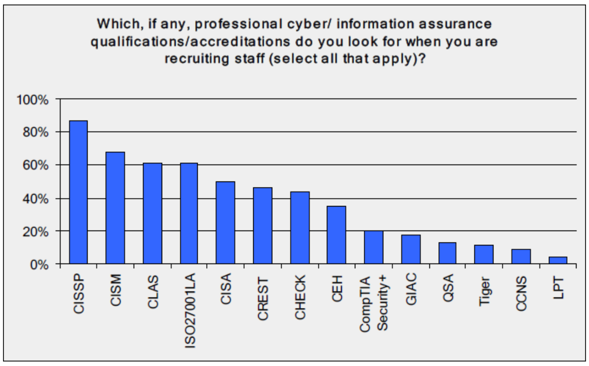

Figure 1. Professional cyber/information assurance qualifications and accreditations (HM Government, 2014, p. 16)

4.7 Servicing

The servicing process should ensure that validated software updates and patches that are used to remediate vulnerabilities are provided.

5 Conclusions

The explosion of the digital landscape increased the need to secure company’s digital property/assets and medical devices from cyberattacks. Finding a balance between increasing development costs and investments in security controls is one of the project management challenges. Software test professionals and IT infrastructure personnel must integrate security testing in their testing procedures as well as to continuously gain knowledge about security testing tools and latest cyber vulnerabilities of hardware and software. To get a proper overview of regulatory requirements that address the security of interconnected medical devices and related software has become increasingly difficult given the number of regulations, standards, frameworks, guidance documents, technical reports, and best practices on this topic. Some standards do not contain explicit provisions on cybersecurity but they provide some guidance for the implementation of security controls.

Cybersecurity has become of paramount importance in the software life cycle processes. Cybersecurity is an iterative process that involves the full product life cycle. When designing a robust cybersecurity program, medical device manufacturers should consider the following key components: 1) designing products from the start with cybersecurity in mind (i.e., prevention), 2) performing security and penetration testing and applying other cybersecurity controls to reduce exploitable weaknesses and attacks (i.e., detection), and 3) having a maintenance plan in place in case of a cyberattack (i.e., incident response and recovery). Implementing a proactive security approach against threats can drive up the value of the company’s products and services.

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 two anonymous reviewers for their valuable comments and suggestions which helped to improve this paper.

References

A Glossary of Common Cybersecurity Terminology. (2017). Retrieved from https://niccs.us-cert.gov/glossary

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

Abbott (St Jude Medical Inc.) 4/12/17. (2017). Retrieved from https://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2017/ucm552687.htm

ANSI/AAMI CI86: Cochlear implant systems: Requirements for safety, functional verification, labeling and reliability reporting. (2017).

Arxan. (2016). 5th Annual State of Application Security Report: Perception vs. Reality.

Best Practices for Security & Privacy. (2016). Retrieved from https://developer.android.com/training/best-security.html

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).

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

CFDA Spells Out Cybersecurity Requirements. (2017). Retrieved from http://www.fdanews.com/articles/180417-cfda-spells-out-cybersecurity-requirements

Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication. (2017). Retrieved from https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm

FDA. (2005). Guidance for Industry – Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software.

FDA. (2014). Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff.

FDA. (2016). Postmarket Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff.

Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication. (2017). Retrieved from https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm

Focus on Cybersecurity. (2017). Retrieved from http://www.abbott.com/corpnewsroom/leadership/focus-on-cybersecurity.html

Goertzel, K. M., Winograd, T., McKinley, H. L., Oh, L., Colon, M., McGibbon, T., Fedchak, E. & Vienneau, R. (2007). Software Security Assurance: A State-of-the-Art Report (SOAR). Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a472363.pdf

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

HM Government. (2014). Cyber Security Skills: Business perspectives and Government's next steps.

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 80001-1: Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities. (2010).

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).

IEC TR 80001-2-9: Application of risk management for IT-networks incorporating medical devices – Part 2-9: Application guidance – Guidance for *use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities*. (2017).

IEC/TR 80001-2-2: Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the communication of medical device security needs, risks and controls. (2012).

ISO 14971: Medical devices – Application of risk management to medical devices. (2007).

ISO 27799: Health informatics – Information security management in health using ISO/IEC 27002. (2016).

ISO/IEC 12207: Systems and software engineering – Software life cycle processes. (2008).

ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary. (2016).

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

ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security controls. (2013).

ISO/IEC 27032: Information technology – Security techniques – Guidelines for cybersecurity. (2012).

ISO/IEC 29147: Information technology – Security techniques – Vulnerability disclosure. (2014).

ISO/IEC 30111: Information technology – Security techniques – Vulnerability handling processes. (2013).

Knott, D. (2015). *Hands-on mobile app testing: a guide for mobile testers and anyone involved in the mobile app business*. Crawfordsville: Addison-Wesley.

KPMG LLP. (2015). Health Care and Cyber Security – Increasing Threats Require Increased Capabilities.

Layered security is IT's best defense. (2016). Retrieved from http://searchmobilecomputing.techtarget.com/tip/Layered-security-is-ITs-best-defense

Medical Devices Hit By Ransomware For The First Time In US Hospitals. (2017). Retrieved from https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#732496df425c

Meeuwisse, R. (2017). *Cybersecurity for Beginners* (Second Edi.). Hythe: Cyber Simplicity Ltd.

Microsoft Security Development Lifecycle. (2017). Retrieved from https://www.microsoft.com/en-us/sdl/

Mobile Top 10 2016-Top 10. (2017). Retrieved from https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

NIST SP 800-30 Revision 1: Guide for Conducting Risk Assessments. (2012).

NIST. (2017). Framework for Improving Critical Infrastructure Cybersecurity. Draft Version 1.1.

Official Journal of the European Union L 117. (2017). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2017:117:FULL&from=EN

OWASP Secure Coding Practices – Quick Reference Guide. (2010).

OWASP Top 10 Application Security Risks – 2017. (2017). Retrieved from https://www.owasp.org/index.php/Top_10_2017-Top_10

Ponemon Institute. (2016). The State of Cybersecurity in Healthcare Organizations in 2016.

Robichau, B. P. (2014). *Healthcare Information Privacy and Security: Regulatory Compliance and Data Security in the Age of Electronic Health Records*. Apress.

Security Hackers Help Bigfoot Biomedical Keep Patient Info Secure. (2017). Retrieved from https://www.youtube.com/watch?v=rz21fb4YVX0&feature=youtu.be

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

Summary of the HIPAA Security Rule. (2013). Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Svensson, R. (2016). *From Hacking to Report Writing: An Introduction to Security and Penetration Testing*. Berlin: Apress.

Top 10 cybersecurity must-haves for 2017. (2017). Retrieved from http://www.distilnfo.com/hitrust/2017/05/11/top-10-cybersecurity-must-haves-2017/

UL 2900 Cybersecurity Standards Set for FDA Adoption. (2017). Retrieved from https://www.emergogroup.com/blog/2017/07/ul-2900-cybersecurity-standards-set-fda-adoption

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

UL 2900-2-1: Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare Systems. (2016).

UL 2900-2-2: Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems. (2016).

Ware, W. H. (1967). Security and Privacy in Computer Systems. The RAND Corporation, Santa Monica, California.

Ware, W. H. (1970). Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security. The Rand Corporation, Santa Monica, California.

Wittkop, J. (2016). *Building a Comprehensive IT Security Program: Practical Guidelines and Best Practices*. Boulder: Apress.