An Overview of Global Professional Publications Related to Medical Device Cybersecurity

Nadica Hrgarek Lechner
University of Zagreb
Faculty of Organization and Informatics
Pavlinska 2, 42000 Varaždin, Croatia
nhrgarek@foi.unizg.hr

Abstract. *The purpose of this paper is to provide an overview of the current professional literature about medical device cybersecurity from a regulatory point of view and at the global level. This paper provides the most comprehensive overview of such publications to date. It may assist healthcare, medical device, regulatory affairs, quality management, and cybersecurity professionals, researchers, regulators, and other subject matter experts in identifying applicable cybersecurity regulations, standards, and industry best practices for medical devices.*

Keywords. cybersecurity, FDA, guidance, medical devices, regulation, standard

1 Introduction

Medical device companies are operating in a highly regulated industry and need to comply with applicable laws and regulations on data privacy protection and cybersecurity. In the past, medical devices were mostly designed and developed as non-networked devices. The main focus was on general safety and performance requirements, and less on security. Nowadays, medical devices often incorporate third-party hardware and software components and we observe an increase in use of wireless, Internet connected, networked, and interconnected medical devices. The expanded use of smartphones, tablets, wearable devices, and cloud services has fostered the development of Internet of Medical Things (IoMT) in the last few years. Due to the growing number of networked medical devices, which can be vulnerable to a wide variety of security threats, medical device manufacturers should address security risk management from initial device conception to disposal. Together, these trends have resulted in an increase in professional publications (i.e., national laws and regulations, standards, guidance documents, technical (information) reports, trend reports, white papers, industry best practices, frameworks, playbooks, information for consumers, etc.) to strengthen cybersecurity requirements for medical devices at the global level.

This paper aims to provide an overview of the current professional publications related to medical device cybersecurity across the globe. Related work is provided in section 2. Section 3 presents the results of conducted narrative literature review. The final section gives a brief summary and discussion of the findings, and identifies areas for further research.

2 Related Work

In 2005, the Food and Drug Administration (FDA), a federal agency of the United States, issued a first guidance document about cybersecurity for networked medical devices containing off-the-shelf software. This guidance (FDA, 2005) recommends validating computer software changes to address cybersecurity vulnerabilities and developing a cybersecurity maintenance plan.

In June 2013, the FDA issued a draft guidance document that addresses management of cybersecurity in medical devices throughout the premarket phase. The final guidance was released by the FDA in October 2014. In this final guidance, the FDA (2014) 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. In October 2018, the FDA updated the premarket guidance. This draft guidance (FDA, 2018) also includes some postmarket recommendations.

In December 2016, the FDA published a second guidance that addresses management of cybersecurity in medical devices during the postmarket phase. According to this guidance (FDA, 2016), cybersecurity applies to the following types of medical devices: a) devices that contain software, firmware, or programmable logic, b) software that is a medical device, including mobile medical applications, c) interoperable devices, and d)

marketed and distributed legacy devices. Over the last three years, many countries around the world published their own regulatory guidelines about cybersecurity of medical devices.

At the moment, there are many standards about information security management and standards covering different aspects of cybersecurity such as vulnerability disclosure, vulnerability handling processes, risk management for IT-networks incorporating medical devices, etc., that can be adopted by medical device manufacturers and healthcare organizations. There is a lack of an international consensus cybersecurity standard that is solely focused on the medical device industry. The International Electrotechnical Commission (IEC), the international standards and conformity assessment body for all fields of electrotechnology, is developing a new standard IEC/DIS 80001-1 (*IEC/DIS 80001-1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software – Part 1: Application of risk management*, 2020) to support medical device manufacturers with respect to security risk management for connected medical devices and connected health software.

While there are many scientific papers about current international standards and trends of medical device cybersecurity, to the best of the author's knowledge, they only focus on: a) one or more professional publications (Anonymous, 2019), (Baranchuk et al., 2018), (Brown et al., 2016), (Jagannathan & Sorini, 2015), (Jump, 2019), (Jump & Finnegan, 2017), (Mankovich & Fitzgerald, 2011), (Murthy, 2019), (Sametinger et al., 2015), (Schwartz et al., 2018), (Stern, 2017), (Stern et al., 2019), (Vargas, 2017), (Walker, 2018), (Wu & Eagles, 2016), b) major countries (Chen et al., 2018), (Fu & Blum, 2013), (Kim et al., 2020), c) a particular geographic area (Abraham et al., 2019), (Best, 2020), (Burns et al., 2016), (Coburn, 2016), (Martinez, 2018), (Owens, 2016), (Pasanisi, 2017), (Pesapane et al., 2018), (Skierka, 2018), (Webb & Dayal, 2017), d) particular types of medical devices (Carroll & Richardson, 2016), (Gladden, 2016), (Hrgarek, 2012), (Hrgarek Lechner, 2017), (Pirker & Hrgarek Lechner, 2019), (Yuan et al., 2018), e) a particular ability of medical devices (Hatcliff et al., 2019), (Hrgarek Lechner, 2018), or f) a particular activity of the cybersecurity process (Arbelaez et al., 2018), (Jiang et al., 2020), (Moshi et al., 2019), (Suárez & Scott, 2017). No paper has been found that provided a comprehensive overview of professional medical device cybersecurity publications at the global level.

3 Narrative Literature Review

The purpose of the conducted narrative literature review was to identify relevant professional publications related to medical device cybersecurity across the globe. The scope of this review was limited to English and German professional publications that were published in the time period from August 1996 to August 2020. August 1996 was chosen because the Health Insurance Portability and Accountability Act of 1996, the U.S. federal law that requires the protection of sensitive patient health information, was published at this time. Literature search was performed using: a) e-mail notifications from FDA and normScan (an online monitoring and tracking tool for new and updated medical device standards), b) searches in IEC and ISO webstores, c) various keyword searches in Google web search engine, and d) content shared on the LinkedIn platform by the TÜV SÜD (a notified body in Germany), the British Standards Institution (the UK national standards body), and regulatory affairs professionals in the medical device industry. Some publications were identified in scientific papers referenced in the previous section.

As listed in Table 1, a total of 156 relevant professional publications addressing cybersecurity for medical devices were searched. This table provides the most comprehensive overview of global professional publications from various sources to date and indicates the complexity of the evolving medical device cybersecurity ecosystem in a highly regulated environment. Since cybersecurity in the medical device industry requires shared responsibility among stakeholders (e.g., medical device manufacturers, healthcare providers, patients, security researchers, etc.), a number of laws, regulations, standards, guidance documents, and other types of publications is currently needed to cover the entire device life cycle.

Maintaining compliance with other regulatory requirements in the medical device industry, such as a risk management process or a usability engineering process, is easier due to a relatively small number of regulations and standards. For example, ISO 14971 (*ISO 14971: Medical devices – Application of risk management to medical devices*, 2019) is an international, harmonized standard for a risk management process that has been specifically designed for the medical device industry. The standard has been recognized as a consensus standard by international regulators such as the FDA and the Australian Therapeutic Goods Administration (TGA).

Table 1. An overview of global professional publications related to medical device cybersecurity

Area/country	Publisher name	Publication title	Publication type	Year
Australia	Therapeutic Goods Administration (TGA)	Medical device cyber security guidance for industry, Version 1.0	Guidance	2019
		Medical device cyber security guidance for	Guidance	2019

Area/country	Publisher name	Publication title	Publication type	Year
		users, Version 1.0		
		Medical device cyber security – Consumer information	Consumer information	2019
Canada	Health Canada	Guidance Document: Pre-market Requirements for Medical Device Cybersecurity	Guidance	2019
China	China Food and Drug Administration (CFDA)	Medical Device Network Security Registration on Technical Review Guidance Principle	Guidance	2017
European Union (EU)	European Parliament and the Council	Directive (EU) 2016/1148 – Measures for a high common level of security of network and information systems across the Union	Directive	2016
		Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR)	Regulation	2016
		Regulation (EU) 2017/745 – Medical Devices Regulation (MDR)	Regulation	2017
		Regulation (EU) 2017/746 – In Vitro Diagnostic Medical Devices Regulation (IVDR)	Regulation	2017
		Regulation (EU) 2019/881 – Cybersecurity Act	Regulation	2019
	European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (COCIR)	Advancing Cybersecurity of Health and Digital Technologies	White paper	2019
	European Committee for Electrotechnical Standardization	EN 45502-1:2015 Implants for surgery – Active implantable medical devices. Part 1: General requirements for safety, marking and for information to be provided by the manufacturer	Standard	2015
	European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures	Information report	2017
		PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS: Good practices for the security of Healthcare services	Guidance	2020
	Medical Device Coordination Group (MDCG)	MDCG 2019-16 - Guidance on Cybersecurity for medical devices	Guidance	2019
France	National Agency for Medicines and Health Products Safety (ANSM)	ANSM's guideline – Cybersecurity of medical devices integrating software during their life cycle[a]	Guidance	2019
Germany	Expertenkreis CyberMed	Sicherheit von Medizinprodukten: Leitfaden zur Nutzung des MDS2 aus 2019	Guidance	2019
	Federal Institute for Drugs and Medical Devices	Das Fast-Track-Verfahren für digitale Gesundheitsanwendungen (DiGA) nach § 139e SGB V: Ein Leitfaden für Hersteller, Leistungserbringer und Anwender	Guidance	2020
	Federal Ministry of Health	Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG)	Law	2019
		Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung – DiGAV)	Regulation	2020
	Federal Office for Information Security (BSI)	BSI-CS 132 Cyber Security Requirements for Network-Connected Medical Devices, Version 1.1	Best practices	2018
		BSI TR-03161 Sicherheitsanforderungen an	Technical	2020

Area/country	Publisher name	Publication title	Publication type	Year
		digitale Gesundheitsanwendungen, Version 1.0	guidance	
	TÜV Rheinland, OpenSky	AN INTRODUCTION TO MEDICAL DEVICE CYBER SECURITY: A European Perspective	White paper	2016
	TÜV Rheinland	Cybersecurity Trends 2018: Cybersecurity in einer zunehmend digitalen Welt	Trend report	2018
		Cybersecurity Trends 2020: New thinking on cybersecurity and privacy in a world where digital transformation beckons	Trend report	2020
	TÜV SÜD, Johner Institute, Dr. Georg Heidenreich	IT Security Guideline for Medical Devices	Guidance	2018
	Verband der Diagnostica-Industrie (VDGH)	IT-Product Security Whitepaper Template, Version 1.4	White paper	2020
International	Advanced Medical Technology Association (AdvaMed)	AdvaMed Medical Device Cybersecurity Foundational Principles	Guidance	2017
	ECRI Institute	Top 10 Health Technology Hazards for 2020	Executive brief	2019
		2019 Top 10 Health Technology Hazard	Executive brief	2018
		Top 10 Health Technology Hazards for 2018	Executive brief	2017
		Top 10 Health Technology Hazards for 2017	Executive brief	2016
		Top 10 Health Technology Hazards for 2016	Executive brief	2015
		Top 10 Health Technology Hazards for 2015	Executive brief	2014
		Top 10 Health Technology Hazards for 2014	Executive brief	2013
		Top 10 Health Technology Hazards for 2013	Executive brief	2012
	EPFL International Risk Governance Center (IRGC)	Governing cybersecurity risks and benefits of the Internet of Things: Connected medical & health devices and connected vehicles	Workshop report	2017
	Frost & Sullivan, Inc.	Medical Device and Network Security: Coming to terms with the Internet of Medical Things (IoMT)	White paper	2019
	Global Digital Health Partnership (GDHP) Cybersecurity Workstream	Medical Device Manufacturer Internet of Things (IoT) Code of Conduct[a]	Guidance	2020
	Healthcare Information and Management Systems Society (HIMSS)	HIMSS Privacy Impact Assessment Guide, Version 2	Guidance	2008
	IEEE Cybersecurity Initiative (CYBSI)	Building Code for Medical Device Software Security	Report	2015
	IEEE Standards Association (SA)	P11073-40102 - IEEE Draft Standard - Health informatics - Device interoperability - Part 40102: Cybersecurity - Capabilities for Mitigation[a]	Standard	2019
	Integrating the Healthcare Enterprise (IHE) Patient Care Device (PCD) Technical Committee	Medical Equipment Management (MEM): Cyber Security, Revision 2.0	White paper	2011
		Medical Equipment Management (MEM): Medical Device Cyber Security – Best Practice Guide, Revision 1.1	White paper	2015
	IHE PCD Technical Committee, Medical Device Innovation, Safety, & Security Consortium (MDISS)	Medical Device Software Patching, Revision 1.1	White paper	2015
	International Electrotechnical Commission (IEC)	IEC 62304:2006 + AMD1:2015 Medical device software – Software life cycle processes	Standard	2015
		IEC/DIS 62304.2 Health software – Software life cycle processes[b]	Standard	---

Area/country	Publisher name	Publication title	Publication type	Year
		IEC 82304-1:2016 Health software – Part 1: General requirements for product safety	Standard	2016
		IEC 80001-1:2010 Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities	Standard	2010
		IEC/DIS 80001-1 Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software – Part 1: Application of risk management	Standard	---
		IEC/TR 80001-2-1:2012 Application of risk management for IT-networks incorporating medical devices – Part 2-1: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples	Technical report	2012
		IEC/TR 80001-2-2:2012 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	Technical report	2012
		IEC/TR 80001-2-3:2012 Application of risk management for IT-networks incorporating medical devices – Part 2-3: Guidance for wireless networks	Technical report	2012
		IEC/TR 80001-2-4:2012 Application of risk management for IT-networks incorporating medical devices – Part 2-4: General implementation guidance for Healthcare Delivery Organizations	Technical report	2012
		IEC/TR 80001-2-8:2016, 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 80001-2-2	Technical report	2016
		IEC/CD 80001-5-1 Safety, security and effectiveness in the implementation and use of connected medical devices or connected health software – Part 5-1: Security Activities in the product lifecycle[b]	Standard	---
		IEC/TR 60601-4-5 ED1 Medical electrical equipment – Part 4-5 Guidance and interpretation – Safety related technical security specifications for medical devices[b]	Technical report	---
	International Organization for Standardization (ISO)	ISO/AWI TS 82304-2 Health software – Part 2: Health and wellness apps – Quality and reliability[b]	Standard	---
		ISO/CD TR 11633-2 Health informatics – Information security management for remote maintenance of medical devices and medical information systems – Part 2: Implementation of an information security management system (ISMS)[b]	Technical report	---
		ISO/DIS 81001-1 Health software and health IT systems safety, effectiveness and security – Part 1: Principles, concepts, and terms[b]	Standard	---
		ISO 13485:2016 Medical devices – Quality management systems – Requirements for regulatory purposes	Standard	2016
		ISO 14971:2019 Medical devices – Application of risk management to medical devices	Standard	2019
		ISO 27799:2016 Health informatics – Information security management in health using ISO/IEC 27002	Standard	2016

Area/country	Publisher name	Publication title	Publication type	Year
		ISO/TR 22696:2020 Health informatics – Guidance on the identification and authentication of connectable Personal Healthcare Devices (PHDs)	Technical report	2020
		ISO/TR 24971:2020 Medical devices – Guidance on the application of ISO 14971	Technical report	2020
		ISO/TR 80001-2-7:2015 Application of risk management for IT-networks incorporating medical devices – Application guidance – Part 2-7: Guidance for healthcare delivery organizations (HDOs) on how to self-assess their conformance with IEC 80001-1	Technical report	2015
		ISO/TS 11633-1:2019 Health informatics – Information security management for remote maintenance of medical devices and medical information systems – Part 1: Requirements and risk analysis	Standard	2019
	ISO, IEC	ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary	Standard	2018
		ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements	Standard	2013
		ISO/IEC CD 27002 Information security, cybersecurity and privacy protection – Information security controls[b]	Standard	---
		ISO/IEC 27003:2017 Information technology – Security techniques – Information security management systems – Guidance	Standard	2017
		ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management	Standard	2018
		ISO/IEC 27017:2015 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services	Standard	2015
		ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity	Standard	2012
		ISO/IEC 27035-1:2016 Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management	Standard	2016
		ISO/IEC 27035-2:2016 Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response	Standard	2016
		ISO/IEC 27039:2015 Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS)	Standard	2015
		ISO/IEC 29134:2017 Information technology – Security techniques – Guidelines for privacy impact assessment	Standard	2017
		ISO/IEC 29147:2018 Information technology – Security techniques – Vulnerability disclosure	Standard	2018
		ISO/IEC 29151:2017 Information technology – Security techniques – Code of practice for personally identifiable information protection	Standard	2017
		ISO/IEC 30111:2019 Information technology – Security techniques – Vulnerability handling processes	Standard	2019
	International Medical Device Regulators	IMDRF Principles and Practices for Medical Device Cybersecurity	Guidance	2020

Area/country	Publisher name	Publication title	Publication type	Year
	Forum (IMDRF)			
	Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC)	Patching Off-the-Shelf Software Used in Medical Information Systems	White paper	2004
	Open Web Application Security Project (OWASP)	OWASP Secure Medical Device Deployment Standard	Standard	2017
Japan	Pharmaceuticals and Medical Devices Agency (PMDA)	Ensuring Cyber Security of Medical Devices	Notification	2015
		Guidance on Ensuring Cyber Security of Medical Device	Guidance	2018
New Zealand	Medical Council of New Zealand	Telehealth	Statement	2020
	Ministry of Health	HISO 10029:2015 Health Information Security Framework	Standard	2015
		HISO 10037.1 Connected Health Architectural Framework	Standard	2010
		HISO 10037.2 Network to Network Interface Specifications	Standard	2010
		HISO 10037.3:2015 User to Network Interface Specifications	Standard	2015
		HISO 10064:2017 Health Information Governance Guidelines	Standard	2017
Republic of Korea	Korea Internet & Security Agency	Cyber Security Guide for Smart Medical Service	Guidance	2018
Saudi Arabia	Saudi Food and Drug Authority (SFDA)	MDS – G36 Guidance to Medical Devices Cybersecurity for Healthcare Providers, Version 1.0	Guidance	2019
		MDS – G37 Guidance to Post-Market Cybersecurity of Medical Devices, Version 1.0	Guidance	2019
		MDS – G38 Guidance to Pre-Market Cybersecurity of Medical Devices, Version 2.0	Guidance	2019
Singapore	Cyber Security Agency of Singapore (CSA)	Security-by-Design Framework, Version 1.0	Framework	2017
	Health Sciences Authority (HSA)	Regulatory Guidelines for Software Medical Devices – A Lifecycle Approach	Guidance	2019
	Enterprise Singapore	TR 67 : 2018 Connected medical device security	Technical reference	2018
Switzerland	eHealth Suisse	Guide for app developers, manufacturers, and distributors	Guidance	2018
		Checklists: Addendum to the guideline for app developers, manufacturers and distributors	Checklist	2018
Taiwan	Ministry of Health and Welfare	Guidance on Management of Cybersecurity in Medical Devices for Manufacturers	Guidance	2019
United Kingdom	British Standards Institution (BSI)	Cybersecurity of medical devices: Addressing patient safety and the security of patient health information	White paper	2017
	Department for Digital, Culture, Media & Sport (DCMS)	Code of Practice for Consumer IoT Security	Guidance	2018
	Imperial College London, Institute of Global Health Innovation	Improving Cyber Security in the NHS	Report	2020
	Medicines and Healthcare products Regulatory Agency (MHRA)	Guidance: Medical device stand-alone software including apps (including IVDMDs), Version 1.06	Guidance	2020
	NHS Digital	Protecting medical devices	Guidance	2019
	Royal Academy of Engineering	Cyber safety and resilience: strengthening the digital systems that support the modern	Report	2018

Area/country	Publisher name	Publication title	Publication type	Year
		economy		
USA	American National Standards Institute (ANSI), Association for the Advancement of Medical Instrumentation (AAMI)	ANSI/AAMI CI86:2017 Cochlear implant systems: Requirements for safety, functional verification, labeling and reliability reporting	Standard	2017
	ANSI, National Electrical Manufacturers Association (NEMA)	ANSI/NEMA HN 1-2019 American National Standard – Manufacturer Disclosure Statement for Medical Device Security	Standard	2019
	ANSI, Underwriters Laboratories (UL)	ANSI/UL 2900-1:2017 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	Standard	2017
		ANSI/UL 2900-2-1:2017 Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems	Standard	2017
	AAMI	AAMI TIR57:2016 Principles for medical device security – Risk management	Technical information report	2016
		AAMI TIR97:2019 Principles for medical device security – Postmarket risk management for device manufacturers	Technical information report	2019
	Carnegie Mellon University	CMU/SEI-2017-SR-022 The CERT® Guide to Coordinated Vulnerability Disclosure	Guidance	2017
	Department of Health and Human Services (DHHS) Office for Civil Rights	HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework	Crosswalk	2016
	Food and Drug Administration (FDA)	Content of Premarket Submissions for Management of Cybersecurity in Medical Devices[a]	Guidance	2018
		Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	Guidance	2014
		Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software	Guidance	2005
		Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices	Guidance	2017
		Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health	Action plan	2018
		Multiple Function Device Products: Policy and Considerations	Guidance	2020
		Postmarket Management of Cybersecurity in Medical Devices	Guidance	2016
		Radio Frequency Wireless Technology in Medical Devices	Guidance	2013
	Healthcare and Public Health Sector Coordinating Council (HSCC)	MEDICAL DEVICE AND HEALTH IT JOINT SECURITY PLAN	Joint security plan	2019
	Health Care Industry Cybersecurity (HCIC) Task Force	REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY	Report	2017
	Healthcare Supply Chain Association (HSCA)	Medical Device and Service Cybersecurity: Key Considerations for Manufacturers & Healthcare Providers	Best practices	2018
		Recommendations for Medical Device Cybersecurity Terms and Conditions	Recommendation document	2018
	Health-ISAC Inc.	Medical Device Security Part 1: Landscape of Global Regulatory Guidance	White paper	2020

Area/country	Publisher name	Publication title	Publication type	Year
	HS Design, Inc.	Cybersecurity in Medical Devices through Full Systems Design Strategies	Best practices	2015
	Medical Device Innovation Consortium (MDIC)	Medical Device Cybersecurity Report: Advancing Coordinated Vulnerability Disclosure	Report	2018
	National Institute of Standards and Technology (NIST)	Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1	Framework	2018
		SP 800-30 Guide for Conducting Risk Assessments, Revision 1	Guidance	2012
		SP 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2	Framework	2018
		SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Revision 1	Guidance	2008
		SP 800-95 Guide to Secure Web Services	Guidance	2007
		SP 800-121 Guide to Bluetooth Security, Revision 2	Guidance	2017
		SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing	Guidance	2011
	NIST, National Cybersecurity Center of Excellence (NCCoE)	SP 1800-1 Securing Electronic Health Records on Mobile Devices	Guidance	2018
		SP 1800-8 Securing Wireless Infusion Pumps in Healthcare Delivery Organizations	Guidance	2018
	Senator Hannah-Beth Jackson	SB-327 Information privacy: connected devices	Senate bill	2018
	Senator Richard Blumenthal	Medical Device Cybersecurity Act of 2017	Congressional bill	2017
	The MITRE Corporation	Medical Device Cybersecurity: Regional Incident Preparedness and Response Playbook, Version 1.0	Playbook	2018
		Rubric for Applying CVSS to Medical Devices, Version 0.12.04	Playbook	2019
	The Office of the National Coordinator for Health Information Technology (ONC)	Guide to Privacy and Security of Electronic Health Information, Version 2.0	Guidance	2015
	United States Government Accountability Office (GAO)	GAO-12-816 MEDICAL DEVICES: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices	Report	2012
	U.S. Department of Health and Human Services (HHS)	Health Information Technology for Economic and Clinical Health (HITECH) Act	Law	2009
		Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)	Law	1996
		Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients	Best practices	2018
		Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”)	Rule	2002
		Health Insurance Reform: Security Standards (“Security Rule”)	Rule	2003
		Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations	Best practices	2018
		Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations	Best practices	2018
		Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, Resources and Templates	Template	2018
	U.S. Department of	Attack Surface: Healthcare and Public Health	Bulletin	2012

Area/country	Publisher name	Publication title	Publication type	Year
	Homeland Security, National Cybersecurity and Communications Integration Center	Sector		
	U.S. Department of Veterans Affairs (VA)	Medical Device Security, Version 1.0	Enterprise design pattern	2017

[a.] Draft

[b.] Under development

Since 2015, there was a significant increase in the number of released professional cybersecurity publications listed in Table 1. As shown in Figure 1, a total of 117 professional cybersecurity publications were issued between 2015 and 2020 (80.7%), another 22 publications were published during 2008-2014 (15.2%), while only six publications were released during 1996-2007 (4.1%). Three publications were published as a draft version and eight publications are under development and have not been published yet.

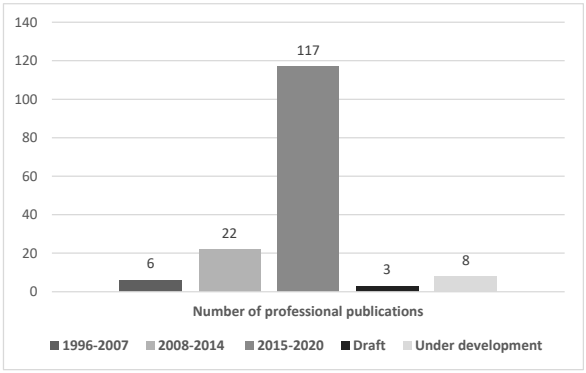

Figure 1. Professional cybersecurity publications by publication timeline

All publications listed in Table 1 were reviewed and classified into 31 different types according to their content. Table 2 lists publication types and shows the number of times they occur in Table 1.

Table 2. Publication types by frequency

Frequency	Publication type
1	Directive, technical guidance, technical reference, information report, workshop report, enterprise design pattern, crosswalk, recommendation document, consumer information, notification, statement, bulletin, joint security plan, action plan, checklist, template
2	Bill (i.e., proposed legislation), rule, technical information report, trend report, playbook
3	Law, framework
5	Regulation
6	Report, best practices
8	Executive brief
10	White paper, technical report
38	Standard
41	Guidance

4 Discussion and Conclusions

This paper has shown that medical device manufacturers operating in global context must tackle a high number of professional cybersecurity publications and different publication types. Since the first FDA's guidance document outlining the agency's cybersecurity expectations from a premarket perspective was published in 2014, many international regulators introduced their own guidance documents.

Due to the increasing number of regulations and regulatory compliance requirements that are sometimes listed within the guidance documents, implementing cybersecurity is very challenging for medical device industry practitioners and other stakeholders. Medical device companies must identify applicable cybersecurity regulations in countries where they plan to market their products and find an effective solution how to comply with applicable cybersecurity regulations and to maintain compliance.

This paper may assist different groups of professionals, researchers, regulators, and other subject matter experts in identifying applicable cybersecurity regulations, standards, and industry best practices for medical devices. Introducing an international standard that is recognised by most international regulators may help to address the challenges from a regulatory point of view.

The main weakness of this paper was that no systematic literature review could be performed due to the nature of professional cybersecurity publications. Only a relatively small number of such publications can be found in academic databases and search engines that are used for finding and accessing scientific papers.

Due to the scope of conducted narrative literature review, only English and German publications were included. Future work should seek to broaden this

further. It would be interesting to develop a centralized database containing a catalogue of applicable professional publications related to medical device cybersecurity. Such database should be extensible with new entries and contain metadata and keywords for easier search. Further research might explore relevant professional publications related to data privacy protection within the medical sector.

Acknowledgments

The author would like to thank the anonymous reviewers for their valuable comments and suggestions that significantly improved this paper.

References

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, 62(4), 539–548.

Anonymous. (2019). The Roundup: A compilation of items about healthcare technology news, regulations, and AAMI initiatives. *Biomedical Instrumentation & Technology*, 53(6), 404–407.

Arbelaez, A., Edwards, S., Littlefield, K., Wang, S., & Zheng, K. (2018). Securing Wireless Infusion Pumps. *Proceedings of the 2018 IEEE Cybersecurity Development (SecDev)* (pp. 141–141). Cambridge.

Baranchuk, A., Refaat, M. M., Patton, K. K., Chung, M. K., Krishnan, K., Kutyifa, V., Upadhyay, G., Fisher, J. D., & Lakkireddy, D. R. (2018). Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know? *Journal of the American College of Cardiology*, 71(11), 1284–1288.

Best, J. (2020). Could implanted medical devices be hacked? *BMJ: British Medical Journal*, 368:m102.

Brown, N. A., Carey, C. H., & Gallant, M. P. (2016). Cybersecurity of Postmarket Medical Devices Addressed by FDA in Draft Guidance. *Intellectual Property & Technology Law Journal*, 28(4), 9–11.

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

Carroll N., & Richardson, I. (2016). Software-as-a-Medical Device: demystifying Connected Health regulations. *Journal of Systems and Information Technology*, 18(2), 186–215.

Chen, Y. J., Chiou, C. M., Huang, Y. W., Tu, P. W., Lee, Y. C., & Chien, C. H. (2018). A Comparative Study of Medical Device Regulations: US, Europe, Canada, and Taiwan. *Therapeutic Innovation & Regulatory Science*, 52(1), 62–69.

Coburn, K. R. (2016). THE INTERNET OF MEDICAL THINGS. *Scitech Lawyer*, 12(3), 18–20.

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.

FDA. (2018). Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Draft Guidance for Industry and Food and Drug Administration Staff.

Fu, K., & Blum, J. (2013). Controlling for Cybersecurity Risks of Medical Device Software. *Communications of the ACM*, 56(10), 21–23.

Gladden, M. E. (2016). Information Security Concerns as a Catalyst for the Development of Implantable Cognitive Neuroprostheses. *Proceedings of the 9th Annual Conference of the EuroMed Academy of Business: Innovation, Entrepreneurship and Digital Ecosystems (EUROMED 2016)* (pp. 891–904). Warsaw.

Hatcliff, J., Zhang, Y., & Goldman, J. M. (2019). Risk Management Objectives for Distributed Development of Interoperable Medical Products. *Proceedings of the 2019 IEEE Symposium on Product Compliance Engineering (SPCE Austin)* (pp. 1–6). Austin.

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

Hrgarek Lechner, N. (2018). Developing a Compliant Cybersecurity Process for Medical Devices. *Proceedings of the Central European Conference on Information and Intelligent Systems (CECIIS)* (pp. 197–204). University of Zagreb, Faculty of Organization and Informatics Varaždin.

Hrgarek, N. (2012). Certification and regulatory challenges in medical device software development. *Proceedings of the 2012 4th*

International Workshop on Software Engineering in Healthcare (SEHC) (pp. 40–43). Zürich.

IEC/DIS 80001-1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software – Part 1: Application of risk management. (2020). Retrieved from https://www.iso.org/standard/72026.html

ISO 14971: Medical devices – Application of risk management to medical devices. (2019).

Jagannathan, S., & Sorini, A. (2015). A cybersecurity risk analysis methodology for medical devices. *Proceedings of the 2015 IEEE Symposium on Product Compliance Engineering (ISPCE)* (pp. 1–6). Chicago.

Jiang, N., Mück, J. E., & Yetisen, A. K. (2020). The Regulation of Wearable Medical Devices. *Trends in Biotechnology*, 38(2), 129–133.

Jump, M. (2019). AAMI TIR97: A Vital Resource in the Postmarket Management of Medical Device Security. *Biomedical Instrumentation & Technology*, 53(6), 462–464.

Jump, M., & Finnegan, A. (2017). Using Standards to Establish Foundational Security Requirements for Medical Devices. *Biomedical Instrumentation & Technology*, 51(s6), 33–37.

Kim, D., Choi, J., & Han, K. (2020). Medical Device Safety Management Using Cybersecurity Risk Analysis. *IEEE Access*, 8, 115370–115382.

Mankovich, N., & Fitzgerald, B. (2011). Managing Security Risks With 80001. *Biomedical Instrumentation & Technology*, 45(s2), 27–32.

Martinez, J. B. (2018). Medical Device Security in the IoT Age. *Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 128–134). New York City.

Moshi, M. R., Parsons, J., Tooher, R., & Merlin, T. (2019). Evaluation of Mobile Health Applications: Is Regulatory Policy Up to the Challenge? *International Journal of Technology Assessment in Health Care*, 35(5), 351–360.

Murthy, V. (2019). Cybersecurity-Related Regulatory Considerations for Medical Devices. *Biomedical Instrumentation & Technology*, 53(4), 312–314.

Owens, B. (2016). Stronger rules needed for medical device cybersecurity. *The Lancet*, 387, 1364.

Pasanisi, J. (2017). China's new cyber law worries market. *International Financial Law Review*. Retrieved from https://search.proquest.com/docview/1962312690?accountid=202211

Pesapane, F., Volonté, C., Codari, M., & Sardanelli, F. (2018). Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. *Insights into Imaging*, 9, 745–753.

Pirker, A., & Hrgarek Lechner, N. (2019). Designing Secure Architecture of Health Software using Agile Practices. *Proceedings of the Central European Conference on Information and Intelligent Systems (CECIIS)* (pp. 269–280). University of Zagreb, Faculty of Organization and Informatics Varaždin.

Sametinger, J., Rozenblit, J., Lysecky, R., & Ott, P. (2015). Security Challenges for Medical Devices. *Communications of the ACM*, 58(4), 74–82.

Schwartz, S., Ross, A., Carmody, S., Chase, P., Coley, S. C., Connolly, J., & Zuk, M. (2018). The evolving state of medical device cybersecurity. *Biomedical Instrumentation & Technology*, 52(2), 103–111.

Skierka, I. M. (2018). The governance of safety and security risks in connected healthcare. *Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT – 2018* (pp. 1–12). London.

Stern, A. D., Gordon, W. J., Landman, A. B., & Kramer, D. B. (2019). Cybersecurity features of digital medical devices: An analysis of FDA product summaries. *BMJ Open*, 9(6), 1–7.

Stern, G. (2017). Getting with the Program to Beef Up Cybersecurity, *Biomedical Instrumentation & Technology*, 51(1), 70–75.

Suárez, R. A., & Scott, D. (2017). Doing What Is Right with Coordinated Vulnerability Disclosure. *Biomedical Instrumentation & Technology*, 51(s6), 42–45.

Vargas, W. (2017). Cybersecurity Standards Are Standing Up to the Bad Actors. *Biomedical Instrumentation & Technology*, 51(s6), 7–8.

Walker, A. (2018). Cybersecurity in safety-critical systems. *Journal of Software: Evolution and Process*, 30(5), e1956.

Webb, T., & Dayal, S. (2017). Building the wall: Addressing cybersecurity risks in medical devices in the U.S.A. and Australia. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 33(4), 559–563.

Wu, F., & Eagles, S. (2016). Cybersecurity for Medical Device Manufacturers: Ensuring Safety and Functionality. *Biomedical Instrumentation & Technology*, 50(1), 23–34.

Yuan, S., Fernando, A., & Klonoff, D. C. (2018). Standards for Medical Device Cybersecurity in 2018. *Journal of Diabetes Science and Technology*, 12(4), 743–746.