EXPLORING MEDICAL DEVICE CYBERSECURITY FROM DESIGN TO POST-MARKET MONITORING

by

MICHAEL OLUWASEUN OGUNDARE

BSc. Hons, The Manchester Metropolitan University, 2008

MS., Minot State University, 2019

MS., Amberton University, 2021

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment for the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA

2024

Exploring medical device cybersecurity from design to post-market monitoring.

Michael Ogundare, *Middle Georgia State University, USA, michael.ogundare@mga.edu*

Abstract

The study aims to improve medical device submission and approval by enhancing cybersecurity risk management. Cybersecurity threats pose significant risks to the safety and integrity of medical devices. Comprehensive cybersecurity risk management and documentation are crucial for regulatory compliance and patient safety. However, inconsistencies in cybersecurity expectations across medical device regulations can lead to gaps in security controls and documentation practices. This study aims to enhance medical device cybersecurity through improved documentation by examining standards and guidelines from regulatory bodies and international organizations. Selected publications from 2015-2023 were analyzed thematically to find cybersecurity documentation themes, best practices, and gaps. The findings suggest that a standardized documentation protocol addressing risk management, incident response, and continuous monitoring can help align cybersecurity practices with device risk levels and regulatory expectations. The study's recommendations for improving documentation transparency and consistency aim to strengthen data security.

Keywords: medical device cybersecurity, cybersecurity risk management, cybersecurity documentation, cybersecurity threats, security controls, risk assessment, incident response, continuous monitoring

Introduction

Cyber threats are a clear danger to medical devices. Comprehensive cybersecurity risk management across a device's lifecycle is crucial for regulatory compliance and safety. Comprehensive cybersecurity risk management and documentation across the product lifecycle is key for compliance and safety. This requires incorporating security controls into design and manufacturing, continuously monitoring threats, and maintaining updated cybersecurity documentation (National Agency for the Safety of Medicines and Health Products, 2019). With rising cyber threats, medical device cybersecurity and documentation should be a top priority for manufacturers seeking to comply with regulations and ensure patient safety.

Robust documentation is crucial for regulatory compliance, audits, and due diligence. It also demonstrates the manufacturer's cybersecurity controls and maintenance procedures (Association for the Advancement of Medical Instrumentation, 2019a; U.S. Food and Drug Administration, 2016; 2023b).

The necessity for proactive security measures in medical devices is clear in light of recent cybersecurity events such as the 2020 ransomware assault on Universal Health Services (Universal Health Services, 2020). Poor credential management, such as default, hard-coded, or readily guessed passwords, can result in unauthorized access (U.S. Food and Drug Administration, 2023b). By establishing comprehensive documentation, manufacturers allow customers to understand cybersecurity risks, integrate devices securely, and operate them according to policies and regulations (National Institute of Standards and Technology, 2020a; U.S. Food and Drug Administration, 2022).

Problem statement

Inconsistent cybersecurity expectations in medical device regulations pose risks to healthcare delivery and patient privacy (National Agency for the Safety of Medicines and Health Products, 2019; Therapeutic Goods Administration, 2022; U.S. Food and Drug Administration, 2022(Haider et al., 2019)). There is a lack of comprehensive cybersecurity information and transparency in device quality systems and approval processes (U.S. Food and Drug Administration, 2023b; Mohammed et al., 2015). This work will provide insights into improving cybersecurity quality systems through enhanced documentation, transparency, and consistent security expectations. Clear guidelines and requirements can close cybersecurity gaps, supporting patient safety and healthcare integrity (Haider et al., 2019).

Purpose of the study

This research aims to enhance medical device data security through improved cybersecurity documentation practices. By examining documentation standards across regulatory bodies such as the like the International Standard Organization – ISO (International Organization for Standardization, 2019), the Food and Drug Administration (U.S. Food and Drug Administration, 2023b), (Association for the Advancement of Medical Instrumentation, 2019c) and the International Medical Device Regulators Forum – IMDRF (Medical Device Cybersecurity Working Group, 2020), this research will identify inconsistencies and best practices.

The findings will provide manufacturers with guidance on optimizing cybersecurity documentation to demonstrate compliance, address risks, and support healthcare delivery integrity. With clearer documentation expectations and requirements, regulators can consistently enforce controls while manufacturers establish more robust cybersecurity protections. The study's analysis of documentation gaps and recommendations for improvement will strengthen data security and patient safety through more transparent and proactive cybersecurity measures. The goal is influencing documentation policies and manufacturer practices to close cybersecurity gaps across medical device lifecycles.

Research questions

Research question 1 (RQ1): How can a uniform cybersecurity documentation protocol be created to address inconsistencies across medical device regulations?

Research question 2 (RQ2): How should cybersecurity documentation requirements align with a medical device’s risk level?

The objectives of the research

The study focused on medical device manufacturers as the population of interest, using guidelines, standards, and regulatory frameworks to understand cybersecurity quality system considerations that manufacturers can use to enhance their cybersecurity risk management procedures.

Review of Literature

Medical device cybersecurity risks can lead to safety issues if breaches cause malfunctions or improper data disclosure (International Organization for Standardization, 2019). Security and safety risks are distinct but interconnected, as vulnerabilities can lead to patient harm (American National Standards Institute., 2016; Association for the Advancement of Medical Instrumentation, 2019b). For instance, a cyberattack that compromises the integrity of a medical device could result in the device malfunctioning and causing harm to a patient. Similarly, unauthorized access to patient data could result in the disclosure of sensitive information that could be used to harm the patient. Comprehensive cybersecurity risk management for

medical devices is needed to address threats to patient safety, business impacts, and compliance (Schist et al., 2022).

However, existing frameworks have gaps in enforcement and oversight of cyber protection. Cybersecurity risk management helps but does not eliminate privacy risk, as privacy problems can arise from non-cyber means. Both cybersecurity and data access/usage must be addressed to fully manage privacy risk (Horák et al., 2019; National Institute of Standards and Technology, 2020b).

There is a lack of in-depth examination on the consistent implementation of robust controls through improved documentation. Prior work shows compliance alone does not guarantee robust defenses, as poor practices like unencrypted devices enabled major breaches (Mohammed et al., 2015). It is advised to go beyond basic compliance by implementing strategic measures such as adopting frameworks, fostering a cybersecurity culture, sharing information, and managing security governance (Cains et al., 2021; Colloud et al., 2023).

Theories and models

Theories posit documentation as a crucial infrastructure shaping the design process (Frith, 2020; Read, 2019; Read & Frith, 2022). Documentation educates stakeholders about security, protects information, maintains trust, and enables regulatory adherence (Dai et al., 2012).

Integrated systems theory analyzes environments and information to determine policies, risk management, controls, and contingencies. Maintaining comprehensive documentation is crucial for regulatory compliance (Hong et al., 2003). Maintaining a comprehensive risk management program with documentation is crucial for complying with laws and regulations, like the FDA's right to refuse policy (U.S. Food and Drug Administration, 2023a).

Methodology

The research followed an adaptation of (Braun & Clarke, 2006; Byrne, 2021) steps for thematic analysis, which involved becoming familiar with the data, creating initial codes, identifying themes, reviewing, and defining themes, and generating an analytical report (McDermott et al., 2022). The research employs an inductive method to analyze the sample data transcripts in the qualitative analysis software (ATLAS.ti Scientific Software Development GmbH, 2024). It searches case-by-case for codes, themes, and categories that emerge from the data. The cases reveal similarities and differences, convergences, and divergences.

Describe the procedure

The study focused on sampling various information-rich, international medical device cybersecurity standards and guidelines published between 2015 and 2023 that are related to medical device cybersecurity (Cousins & Bourgeois, 2014). Table 1 includes standards, technical recommendations, and guidance used in the research.

Table 1: Medical Device Cybersecurity Across Major International Organizations for Standardization and Regulatory Bodies

Authoring Body	Title	Reference
International Electrotechnical Commission	IEC 81001-5-1:2021 Health software and health IT systems safety, effectiveness, and security — Part 5-1: Security — Activities in the product life cycle.	(International Electrotechnical Commission, 2021)
International Medical Device Regulators Forum	Principles and practices for medical device cybersecurity	(Medical Device Cybersecurity Working Group, 2020)
Therapeutic Goods Administration	Medical device cyber security: Guidance for industry (Version 1.2)	(Therapeutic Goods Administration, 2022)
U.S. Food and Drug Administration	Postmarket management of cybersecurity in medical devices: Guidance for industry and Food and Drug Administration staff.	(U.S. Food and Drug Administration, 2016)

A thorough reading of each document was conducted to familiarize the researcher with the content and context (Khan & VanWynsberghe, 2008). This critical first step facilitates the subsequent data analysis process followed by the steps in Table 2. The steps for data analysis in relation to a text-based case study method focusing on cybersecurity in medical devices (Halkias et al., 2023; Maguire & Delahunt, 2017).

Table 2: Coding Scheme Development

Step	Description
Coding Scheme Development	Develop an initial coding scheme derived from a preliminary review of the data sources, identifying, and categorizing key features within the texts.
Iterative Refinement of Coding Scheme	Continually refine and expand the coding scheme as a deeper understanding of the data is achieved, ensuring its relevance and comprehensiveness.
Implementation of Coding Scheme	Apply the refined coding scheme to the entire dataset using qualitative data analysis software, facilitating an organized and systematic approach to coding.
Broader Contextual Analysis	Consider the broader contexts within which these standards and guidelines are implemented, including regulatory, technological, and health care contexts, providing a more comprehensive understanding of the data.

Cross-case synthesis involves comparing and contrasting cases rather than just analyzing individual cases. The cross-case synthesis technique collects findings from multiple individual cases, handling each case separately (Halkias et al., 2023; Onwuegbuzie & Weinbaum, 2016).

Identify data

The data corpus included standards, special publications and guidelines published between 2015 and 2024 related directly to medical device cybersecurity. Table 3 details the nature and scope of the inclusion and exclusion criteria guiding the selection.

Table 3: Document Selection Inclusion and Exclusion Criteria to Enhance Relevancy and Quality

Inclusion Criteria	Exclusion Criteria
From recognized standards (e.g., ISO, FDA, TGA)	From an unknown or non-authoritative source
Published in English	Not in English
Published between 2015-2024	Published outside 2015-2024
Full text available	Full text unavailable
Addresses cybersecurity risk management	Does not address cyber risk management
Relevant to various medical devices	Pertains to specific medical device
Discusses patient safety in cybersecurity	Does not discuss patient safety
Addresses technical and organizational cybersecurity aspects	Addresses only one aspect of cybersecurity

By focusing on these criteria, which are critical to ensure the relevancy and quality of the data, the study gain valuable insights into cybersecurity documentation practices in the medical device industry (Vrhovec et al., 2020). The sampling unit for the case study on medical device cybersecurity were international standards organizations (ISO/IEC), and (Association for the Advancement of Medical Instrumentation), regulatory agencies (FDA), (Therapeutic Goods Administration), and information and guidance from IMDRF involved in regulating and overseeing medical device cybersecurity.

Develop the measure (protocol)

The research requires two-level data analysis. To understand medical device cybersecurity standards from government agencies and international standard organizations at the case level, thematic content analysis, merging information, and triangulating data were needed. The second level is cross-case analysis, which identifies similarities and differences between the three cases and merges the data to reach convergent findings (Tsortanidou et al., 2022).

This data analysis process aims to gain a holistic understanding of cybersecurity's role in securing medical devices throughout their lifecycle, from premarket to post-market. This approach enables an in-depth exploration of the field, thereby identifying best practices, potential gaps, and opportunities for improvement.

Validity

To ensure the validity of the study, the findings were validated by doctoral cohorts' peer review and medical device cybersecurity expert. This involves sharing the findings with experts in the field and seeking their feedback, which are, at the very least, provided a unique perspective (Boyd et al., 2023; Sjøberg & Bergersen, 2023). The research used multiple and reliable sources of data that are relevant to the research question to enhance construct validity. Researcher bias was decreased through clear documentation of techniques, and the use of diverse data sources, and iterative analysis to promote validity (Khan & VanWynsberghe, 2008; Onwuegbuzie & Weinbaum, 2016).

Significance

With connected medical devices, cybersecurity vulnerabilities pose serious risks to patient care systems. Addressing gaps in manufacturer guidance and implementing best practices is crucial for strengthening defenses (Carello et al., 2023; Lottes et al., 2022).

Limitations

Potential limitations encompass the risk of decontextualization of cases and obscuring specific details and nuances of individual scenarios during the comparison process. This was be mitigated by providing rich contextual information for each case, as suggested by Khan and VanWynsberghe (2008). It is acknowledged that this study is limited to standards and guidelines published in English between 2015 and 2024. Therefore, the findings may not be applicable to standards or guidelines published in other languages or outside this time frame.

Results

The thematic visualization (Figure 1) effectively illustrates the relationships between the main themes and their corresponding subthemes identified in the thematic analysis of medical device cybersecurity.

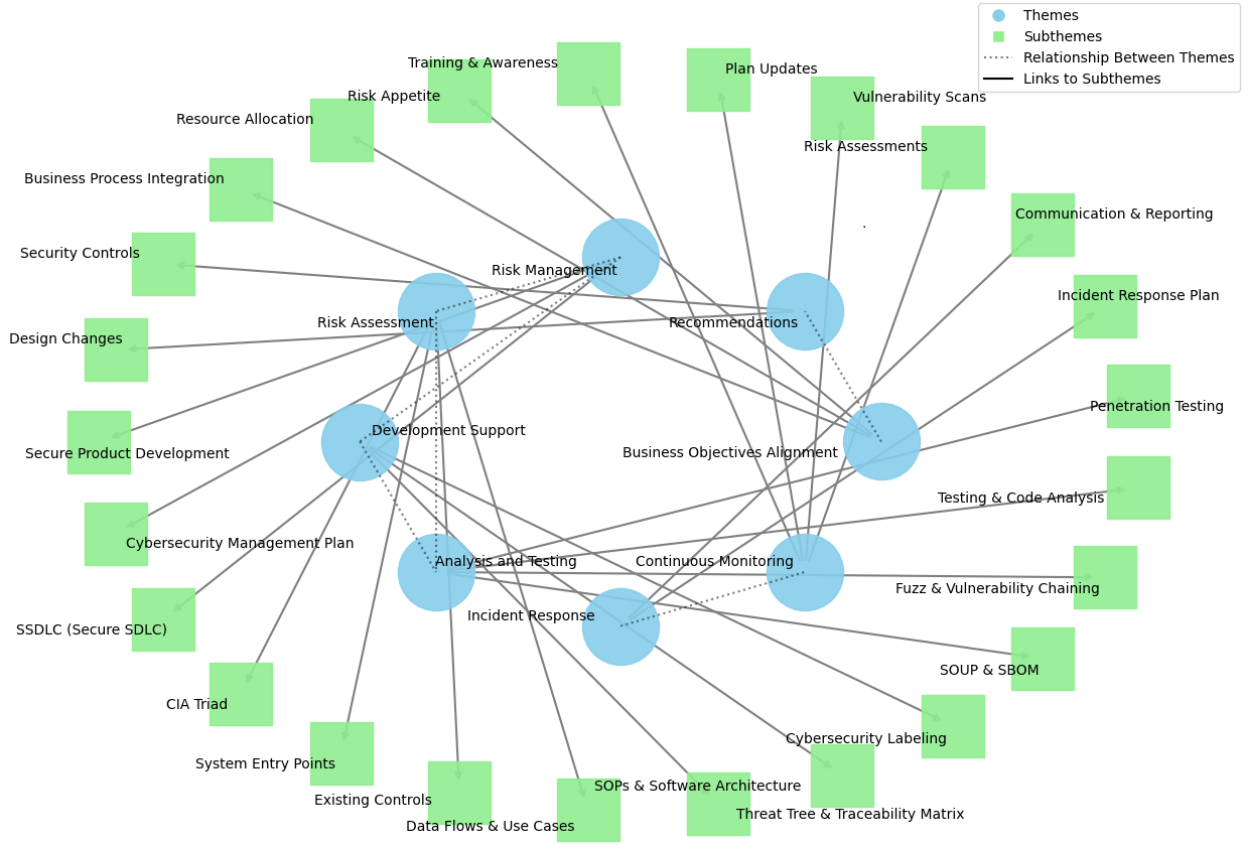

Figure 1: Medical Device Cybersecurity: A Thematic Framework Analysis

The eight main themes are Risk Management, Risk Assessment, Development Support, Analysis and Testing, Incident Response, Continuous Monitoring, Recommendation, and Business Objectives Alignment. Each main theme is connected to its corresponding subthemes, providing a clear visual representation of the framework's structure and organization.

The risk management theme emphasizes the importance of secure product development practices, the establishment of a cybersecurity management plan, and the integration of security considerations throughout the Software Development Life Cycle (SSDLC). The Risk Assessment theme focuses on identifying and evaluating potential security risks by considering the CIA triad, system entry points, existing controls, and detailed data flow and use case analyzes.

The theme of "Development Support" highlights the significance of processes such as threat modeling, traceability matrices, standard operating procedures (SOPs), software architecture considerations, and cybersecurity labeling requirements. The analysis and testing theme encompass rigorous testing procedures, including SOUP analysis, SBOM examination, fuzz testing, vulnerability chaining, code analysis, and penetration testing, to uncover and mitigate vulnerabilities.

Figure 2: Sankey Diagram of Cybersecurity Documentation for Submission

The Sankey diagram (Figure 2) illustrates the complex interconnections between key cybersecurity documentation nodes and their corresponding industry standards and guidelines. The diagram reveals that the "Cybersecurity Risk Management Report" node is linked to multiple standards, including the "FDA Premarket Cybersecurity Guidance," "ISO 14971:2019," and "AAMI TIR57:2016." Similarly, the "Threat Model" node is connected to the "STRIDE Methodology" and "AAMI TIR57:2016."

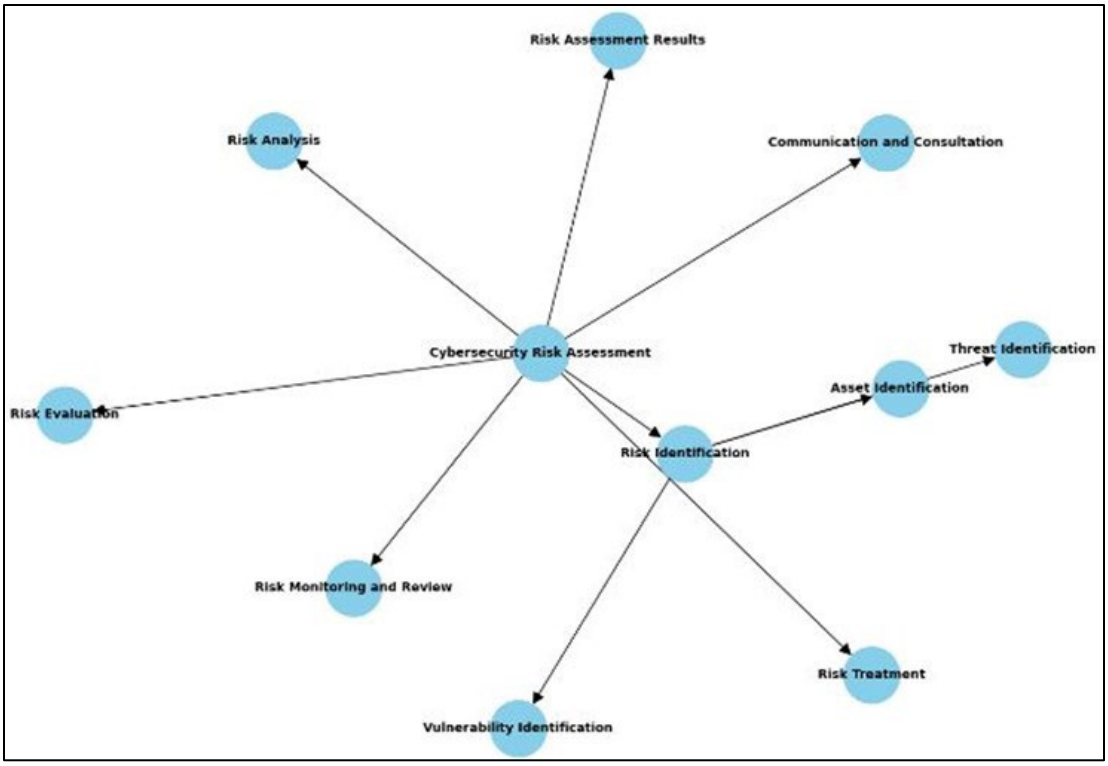

Figure 3: Concept Map for Medical Device Cybersecurity Risk Assessment

The concept map for a cybersecurity risk assessment (Figure 3) serves as a visual representation of the key themes and their interconnections within the realm of medical device cybersecurity documentation. This hierarchical visualization aids stakeholders in comprehending the comprehensive scope of cybersecurity preparedness, ensuring that medical devices are developed, evaluated, and monitored with a robust security posture that aligns with regulatory requirements and industry best practices.

Discussion

The thematic analysis and Sankey diagram emphasize the importance of a comprehensive approach to medical device cybersecurity. The framework highlights the need for risk identification and mitigation throughout the device lifecycle, from development to ongoing monitoring. In Figure 1, the Development Support and Analysis and Testing themes underscore the significance of integrating cybersecurity best practices into the software development process and conducting rigorous testing to uncover vulnerabilities. Whereas, the Incident Response and Continuous Monitoring themes stress the importance of preparedness and ongoing vigilance, while Business Objectives Alignment ensures that cybersecurity efforts align with the organization's overall risk appetite and business processes.

The insights gained from this analysis contribute to the growing body of knowledge in medical device cybersecurity and can serve as a foundation for future research and industry best practices. As the threat landscape evolves, ongoing collaboration between stakeholders will be essential to ensure the safety and security of medical devices.

The Sankey diagram (Figure 2) illustrates that the "Cybersecurity Risk Management Report" is a comprehensive document submitted to regulatory authorities for compliance and approval of medical device cybersecurity. The report consolidates all the essential artifacts, such as the Threat Model,

Cybersecurity Risk Assessment, Interoperability Considerations, Third-Party Software Components, and other crucial elements, as depicted in the diagram. The visual representation highlights the connections between these artifacts and relevant industry standards and guidelines, including the FDA Premarket Cybersecurity Guidance, ISO 14971:2019, and AAMI TIR57:2016, demonstrating the report's adherence to regulatory requirements and best practices.

It illustrates the structured approach to identifying and addressing potential cyber threats, where the central node, 'Cybersecurity Risk Assessment', branches out into core thematic areas like 'Risk Identification', 'Risk Analysis', 'Risk Evaluation', 'Risk Treatment', and others. These themes are further decomposed into more specific elements, such as 'Asset Identification', 'Threat Identification', and 'Vulnerability Identification', representing a granular view of the assessment process.

In conclusion, the findings emphasize the importance of a comprehensive approach that encompasses risk management, assessment, development support, testing, incident response, and continuous monitoring. The interconnectedness of cybersecurity documentation and its alignment with industry standards demonstrate the need for a holistic approach to regulatory compliance. The structured nature of cybersecurity risk assessment, focusing on risk identification, analysis, evaluation, and treatment, is also highlighted. These insights contribute to the growing body of knowledge in medical device cybersecurity and serve as a foundation for future research and industry best practices.

References

American National Standards Institute. (2016). *AAMI TIR57: 2016 - Principles for medical device security - Risk management.* Retrieved October 10, 2023, from https://webstore.ansi.org/standards/aami/aamitir572016?gclid=Cj0KCQjw1aOpBhCOARIsACXYv-f3SYqRhRJn6xnBBr_uQriG1irXJAit-78ZorAs0bGsQGKn90ejW0IaAh2mEALw_wcB

Association for the Advancement of Medical Instrumentation. (2019a). *AAMI TIR57:2016 (R2019): Principles for medical device security - Risk management*. AAMI. Retrieved October 21, 2023, from https://webstore.ansi.org/standards/aami/aamitir572016r2019

Association for the Advancement of Medical Instrumentation. (2019b, September 27). *AAMI TIR97:2019(R2023): Principles for medical device security—Postmarket risk management for device manufacturers*. AAMI. Retrieved October 21, 2023, from https://www.aami.org/detail-pages/product/aami-tir972019-r-2023-pdf-a152e000006j60oqaa

Association for the Advancement of Medical Instrumentation. (2019c, September 27). *AAMI TIR97:2019(R2023): Principles for medical device security—Postmarket risk management for device manufacturers*. AAMI. Retrieved October 21, 2023, from https://www.aami.org/detail-pages/product/aami-tir972019-r-2023-pdf-a152e000006j60oqaa

ATLAS.ti Scientific Software Development GmbH. (2024, February). *ATLAS.ti Mac (version 23.2.1) [Qualitative data analysis software]*. ATLAS.ti. https://atlasti.com

Boyd, R. J., Harvey, M., Roy, D. B., Barber, T., Haysom, K. A., Macadam, C. R., Morris, R. A., Palmer, C., Palmer, S., Preston, C. D., Taylor, P., Ward, R., Ball, S. G., & Pescott, O. L. (2023). Causal inference and large-scale expert validation shed light on the drivers of sdm accuracy and variance. *Diversity and Distributions*, *29*(6), 774–784. https://doi.org/10.1111/ddi.13698

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Byrne, D. (2021). A worked example of braun and clarke's approach to reflexive thematic analysis. *Quality & Quantity*, *56*(3), 1391–1412. https://doi.org/10.1007/s11135-021-01182-y

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2021). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, *42*(8), 1643–1669. https://doi.org/10.1111/risa.13687

Carello, M., Spaccamela, A., Querzoni, L., & Angelini, M. (2023). A systematization of cybersecurity regulations, standards and guidelines for the healthcare sector. *arXiv*. Retrieved May 27, 2023, from https://doi.org/10.48550/arxiv.2304.14955

Colloud, S., Metcalfe, T., Askin, S., Belachew, S., Ammann, J., Bos, E., Kilchenmann, T., Strijbos, P., Eggenspieler, D., Servais, L., Garay, C., Konstantakopoulos, A., Ritzhaupt, A., Vetter, T., Vincenzi, C., & Cerreta, F. (2023). Evolving regulatory perspectives on digital health technologies for medicinal product development. *npj Digital Medicine*, *6*(1). https://doi.org/10.1038/s41746-023-00790-2

Cousins, J., & Bourgeois, I. (2014). Cross-case analysis and implications for research, theory, and practice. *New Directions for Evaluation*, *2014*(141), 101–119. https://doi.org/10.1002/ev.20078

Dai, W., Zhu, Q., Wang, C., & Zeng, Y. (2012). Risk management model of information security in ic manufacturing industry. *Journal of Computers*, *7*(2). https://doi.org/10.4304/jcp.7.2.317-324

Frith, J. (2020). Technical standards and a theory of writing as infrastructure. *Written Communication*, *37*(3), 401–427. https://doi.org/10.1177/0741088320916553

Haider, N., Gates, C., Sengupta, V., & Qian, S. (2019). Cybersecurity of medical devices: Past, present, and future. In T. R. Deer, J. E. Pope, T. J. Lamer, & D. Provenzano (Eds.), *Deer's treatment of pain* (pp. 811–820). Springer International Publishing. https://doi.org/10.1007/978-3-030-12281-2_100

Halkias, D., Neubert, M., & Harkiolakis, N. (2023). Multiple case study data analysis for doctoral researchers in management and leadership. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4423757

Hong, K., Chi, Y., Chao, L. R., & Tang, J. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, *11*(5), 243–248. https://doi.org/10.1108/09685220310500153

Horák, M., Stupka, V., & Husák, M. (2019). GDPR compliance in cybersecurity software: A case study of DPIA in information sharing platform. *ARES '19: 14th International Conference on Availability, Reliability and Security*. http://dx.doi.org/10.1145/3339252.3340516

International Electrotechnical Commission. (2021, December). *IEC 81001-5-1:2021 Health software and health IT systems safety, effectiveness and security - part 5-1: Security - activities in the product life cycle*. ISO. https://www.iso.org/standard/76097.html

International Organization for Standardization. (2019, December). *ISO 14971:2019: Medical devices - Application of risk management to medical devices*. Retrieved October 21, 2023, from https://www.iso.org/standard/72704.html

Khan, S., & VanWynsberghe, R. (2008). View of cultivating the under-mined: Cross-case analysis as knowledge mobilization. *Forum: Qualitative Social Research*, *9*(1). https://doi.org/10.17169/fqs-9.1.334

Lottes, A. E., Cavanaugh, K. J., Chan, Y.-F., Devlin, V. J., Goergen, C. J., Jean, R., Linnes, J. C., Malone, M., Peat, R., Reuter, D. G., Taylor, K., & Wodicka, G. R. (2022). Navigating the regulatory pathway for medical devices—a conversation with the fda, clinicians, researchers, and industry experts. *Journal of Cardiovascular Translational Research*, *15*(5), 927–943. https://doi.org/10.1007/s12265-022-10232-1

Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *All Ireland Journal of Higher Education*, *3*, 3351–33514.

McDermott, O., Foley, I., Antony, J., Sony, M., & Butler, M. (2022). The impact of industry 4.0 on the medical device regulatory product life cycle compliance. *Sustainability*, *14*(21), 14650. https://doi.org/10.3390/su142114650

Medical Device Cybersecurity Working Group. (2020). *Principles and practices for medical device cybersecurity*. International Medical Device Regulators Forum. https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf

Mohammed, D., Mariani, R., & Mohammed, S. (2015). Cybersecurity challenges and compliance issues within the U.S. healthcare sector. *International Journal of Business and Social Research*, *05*(02). Retrieved September 22, 2023, from https://thejournalofbusiness.org/index.php/site/article/view/714/502

National Agency for the Safety of Medicines and Health Products. (2019, July). *ANSM's guideline - cybersecurity of medical devices integrating software during their life cycle* [PDF]. Retrieved February 18, 2024, from https://ansm.sante.fr/uploads/2020/10/16/20201016-pi-190719-cybersecurite-recommandations-eng.pdf

National Institute of Standards and Technology. (2020a). Retrieved February 18, 2024, from https://pages.nist.gov/IoT-Device-Cybersecurity-Requirement-Catalogs/nontechnical/manufacturer/documentation/

National Institute of Standards and Technology. (2020b, January 16). *NIST privacy framework: A tool for improving privacy through enterprise risk management, version 1.0*. Retrieved October 10, 2023, from https://doi.org/10.6028/NIST.CSWP.01162020

Onwuegbuzie, A. J., & Weinbaum, R. K. (2016). Mapping miles and huberman's within-case and cross-case analysis methods onto the literature review process. *Journal of Educational Issues*, *2*(1), 265. https://doi.org/10.5296/jei.v2i1.9217

Read, S. (2019). The infrastructural function: A relational theory of infrastructure for writing studies. *Journal of Business and Technical Communication*, *33*(3), 233–267. https://doi.org/10.1177/1050651919834980

Read, S., & Frith, J. (2022). Introduction. *Communication Design Quarterly*, *10*(3), 5–9. https://doi.org/10.1145/3507870.3507871

Schiestl, R., Hoyme, K., & Aerts, B. (2022). Medical device product security. In W. D. & P. I. (Eds.), *Medical device innovation handbook* (9.0th ed.). University of Minnesota. https://pressbooks.umn.edu/mdih/chapter/medical-device-product-security/

Sjøberg, D. K., & Bergersen, G. (2023). Construct validity in software engineering. *IEEE Transactions on Software Engineering*, *49*(3), 1374–1396. https://doi.org/10.1109/tse.2022.3176725

Therapeutic Goods Administration. (2022, November 8). *Medical device cyber security guidance for industry v1.2*. Retrieved October 21, 2023, from https://www.tga.gov.au/sites/default/files/medical-device-cyber-security-guidance-industry.pdf

Tsortanidou, X., Daradoumis, T., & Barberá-Gregori, E. (2022). Unplugged computational thinking at k-6 education: Evidence from a multiple-case study in spain. *Education 3-13*, *51*(6), 948–965. https://doi.org/10.1080/03004279.2022.2029924

U.S. Food and Drug Administration. (2016). *Postmarket management of cybersecurity in medical devices: Guidance for industry and Food and Drug Administration staff*. Retrieved October 21, 2023, from https://www.fda.gov/files/medical%20devices/published/Postmarket-Management-of-Cybersecurity-in-Medical-Devices---Guidance-for-Industry-and-Food-and-Drug-Administration-Staff.pdf

U.S. Food and Drug Administration. (2022, April 21). *Refuse to accept policy for 510(k)s - guidance for industry and fda*. Retrieved February 18, 2024, from https://www.fda.gov/regulatory-information/search-fda-guidance-documents/refuse-accept-policy-510ks

U.S. Food and Drug Administration. (2023a, March 30). *Cybersecurity in medical devices: Refuse to accept policy for cyber devices and related systems under Section 524B of the FD&C Act [Docket No. FDA-2023-D-1030] [Policy/Guidance document]*. Retrieved October 21, 2023, from https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-refuse-accept-policy-cyber-devices-and-related-systems-under-section

U.S. Food and Drug Administration. (2023b, September 27). *Cybersecurity in medical devices: Quality system considerations and content of premarket submissions: Guidance for industry and Food and Drug Administration staff*. Retrieved October 21, 2023, from https://www.fda.gov/media/119933/download

Universal Health Services. (2020, October 29). *Statement from Universal Health Services*. Retrieved February 18, 2024, from https://uhs.com/statement-from-universal-health-services/

Vrhovec, S., Fujs, D., Jelovcan, L., & Mihelic, A. (2020). Evaluating case study and action research reports: Real-world research in cybersecurity. *JUCS - Journal of Universal Computer Science*, *26*(7), 827–853. https://doi.org/10.3897/jucs.2020.045