

Software as a Medical Device (SaMD): Useful or Useless Term?

Rebecca Hermon
Flinders University
rebecca.hermon@flinders.edu.au

Patricia A H Williams
Flinders University
trish.williams@flinders.edu.au

Vincent B McCauley
Flinders University
vincem@mccauleysoftware.com

Abstract

Software as a medical device is a relatively new and expanding field in which patient safety must be a key concern. Regulation and standards regarding software as a medical device (subsequently referred to as “SaMD”) must incorporate all components that could potentially influence SaMD, both in its development and implementation. However, SaMD has been varyingly defined by organisations and individuals within the literature, therefore there is no clear boundary as to what is or is not SaMD, consequently, no clear definition of SaMD exists. Without a clear definition it therefore becomes impossible to create standards to regulate SaMD. Ultimately, this results in increased risks to patient safety. The purpose of this study was to identify SaMD concepts through a Scoping Review to establish the boundaries of SaMD. This has significant impact on new technology applications to support healthcare monitoring and healthcare service delivery. This will ultimately affect how new technology can be regulated in healthcare and will impact innovation and design in this field.

1. Introduction

The topic of this scoping review is Software as a Medical Device (SaMD), which is primarily the use of computer software applications and mobile applications for health monitoring and management. This scoping review begins with an introduction to SaMD, specifically drawing attention to assessing current definitions. The challenges in defining the boundaries for SaMD and correlating these with the definitions, provides the context for the subsequent discussion of the literature. Medical apps are an important component of this context and their role in SaMD is explored. The scoping review will also discuss medical device software failures, and critically analyse potential solutions involving standards. Following the introduction to SaMD, the review describes the methods used, the results, the outcome and the significance of this research.

1.1. What is SaMD?

The right shift in the population age distribution has resulted in a demand for more effective health systems [1]. This challenge can be addressed through the integration of health information systems and health technologies. These systems play a beneficial role in patient safety, can potentially reduce healthcare costs [2] and are supported by continuing development in the medical devices field [3]. Similarly, Software as a Medical Device, otherwise known as SaMD, is a growth area of health technologies, and is predicted to continue its expansion within the clinical environment. Nonetheless, a number of studies have highlighted the current limitations of SaMD [20]. The main constraint on the depth of work in this area is the lack of an universal definition or agreement as to what SaMD includes or does not include. Many of the main commentators in this field are concerned with this lack of consensus and have attempted to create a definition which can be agreed upon. For example, ISO/IEC 80001 *Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities* has defined medical device software as a “software system that has been developed for the purpose of being incorporated into the medical device or that is intended for use as a medical device in its own right” [3, p.12]. This research does not use this definition because it specifically relates to software that is used within a medical device to function. An alternative definition which has gained traction, has been suggested recently by the International Medical Device Regulators Forum (IMDRF) as “software intended to be used for one or more medical purposes that perform without being part of a hardware medical device” [5, p.6]. Interestingly, the Australian Therapeutic Goods Administration, United States Food and Drug Administration and Canada Health reference the IMDRF definition and have not created their own definition. By comparison, organisations such as the regulators in the European Union, the Asian

Harmonization Working Party, the Chinese Food and Drug Administration, and the Japanese Ministry of Health, Labour and Welfare, are currently developing their own SaMD definitions, standards and regulations. According to the IMDRF definition, clinical software that assists in the diagnosis, treatment, prevention or mitigation of a disease is considered SaMD; however, it is asserted that this definition does not recognise medical devices that were previously not intended for medical purposes, and were unintentionally transformed into a device for medical purpose. Additionally, the IMDRF definition is not fit for purpose as it does not provide a clear definition for software developers and may include desktop information systems such as those used for electronic medical records (EMRs). As a result, the failure to develop an agreed SaMD definition has clear implications for the boundaries and standards of SaMD.

2. The Gap in the Literature

A review of the literature has identified gaps in the development of a definition of SaMD, which makes it difficult to assess SaMD as an effective tool in the delivery of healthcare. Currently, there is no standard definition for SaMD, and no established boundaries for SaMD. This consequently has direct impact on the development of standards for SaMD, as without a concise and agreed definition, affirmed standards cannot be aligned. This has further implications for the creation of new technology applications to support healthcare monitoring, and healthcare service delivery, in relation to how new technology can be regulated as well as the impact on innovation and design. Further, whilst mobile apps are increasingly popular, it is acknowledged that medical apps may not form a part of SaMD, and therefore not be considered regulated devices; even though they may be used for a medical purpose. This can have potentially detrimental and even fatal consequences, as a lack of standardisation of medical apps may result in no regulation of the software development lifecycle for such apps; ultimately, this potentially results in increased risks to patient safety. As a response to this gap, the following research question were developed.

3. Research Questions

1. Can a definition of SaMD be defined that articulates the boundaries of SaMD?
2. What are the factors that impact the definition of SaMD boundaries?

The research questions required analysis of the SaMD literature and references to identify if boundaries can be defined, as well as how they can assist in the creation of an agreed SaMD definition. An analysis of the literature on medical apps and health information systems was undertaken to identify the potential boundaries of SaMD, and how the creation of standards can be used in the development and use of SaMD. As a result, established boundaries of SaMD may result in a framework that could be used to assure patient safety when using SaMD.

4. Research Method

A scoping review method was chosen to answer the research questions, as this method provides the ability to identify key concepts and definitions in the literature [41]. Subsequently, objectives for the scoping review were developed from the Research Questions. These were:

- Research and analyse current literature on SaMD.
- Research and identify the key elements of SaMD which are currently missing from the literature.
- Identify the boundaries of SaMD.

Further sub-questions were developed to assist with answering both the Objectives and Research Questions.

- What is SaMD?
- What are the boundaries of SaMD?
- What are medical apps, and how do they relate to SaMD?
- How is SaMD used?
- Software failure in SaMD
- What are the standards and solutions for software failure in SaMD?

4.1. Criteria and Identifying Relevant Work

Relevant academic articles meeting the inclusion criteria were used to create the categories of SaMD. Appropriate papers were decided on by evaluating each article to determine its academic quality and whether the content related to the area of SaMD. Articles that met the criteria of academic quality included articles that had been peer reviewed, published within the last 20 years, and held validity and reliability. It is important to note that papers older than 20 years were included as pre-literature, and were

identified as foundational papers significant to the research.

Subsequently, a collection of published works were used to determine what components are mentioned and used in SaMD. The final step of the scoping review encompassed the identification of the categories to inform the boundaries of SaMD.

A search term strategy, which involved searching the literature based on relevant key terms, was conducted [42]. The key search terms were derived from concept mapping the keywords and synonyms of SaMD. The following key search terms were used:

- SaMD
- Software as a Medical Device
- Medical Device Software
- Software as a Medical Device and information flow
- Software as a Medical Device consequences
- Software as a Medical Device and risks
- Software as a Medical Device standards
- Medical apps
- Software as a Medical Device Security.

4.2. Assessing Study Quality

Literature articles in suitable databases that met the initial search criteria, that were content relevant and identified as research with rigour were identified. Eleven databases were searched including Proquest, Academic One File, and IEEE. The majority of the literature returned were journal articles; nonetheless online books, standards and published research papers were also examined.

To ensure academic rigour, only articles that had been peer reviewed, and had met the content criteria were selected, and duplicate articles were eliminated. The search of the literature resulted in 145 journal articles, 124 of which were assessed as meeting the criteria for this scoping review.

4.3. Summarising the Evidence

The 124 literature articles selected were critically analysed and the information from these articles was aggregated. The outcome of aggregation resulted in literature categorisations based on the research sub-questions. Table 1 provides the number of articles identified from the research terms.

Remarkably, no relevant search results were found using key search terms “SaMD” or “medical device software”. Of the 124 articles selected, 43 results originated from Proquest, 9 originated from Academic One file, 18 originated from IEEE, 7 originated from Springer Link, 5 originated from Google Scholar, 4 originated from Science Direct, 5 originated from Wiley Online, 4 originated from BMJ, 2 originated from JAMA, 10 originated from PMC, 3 originated from Taylor & Francis and 14 originated from other sources.

Table 1. Articles found from the Research Terms

Research Terms	Total Articles
SaMD	0
Software as a Medical Device	37
Software as a Medical Device Consequences	1
Software as a Medical Device information flow	6
Software as a Medical Device and risks	3
Software as a Medical Device and Standards	10
Medical apps	34
Software as a Medical Device Security	33
Total	124

5. Results

The findings from the scoping review indicate that there is a lack of academic research in the literature using the acronym “SaMD”. It can be argued, SaMD is a relatively new field, which may explain the lack of literature to be found from this specific acronym term. Further, the articles analysed were found to have three primary themes: Software, Standards and Regulation, and Risk Management. The next section describes the themes, and sub-themes identified in the literature.

5.1. Software

The theme Software incorporates sub-themes on functionality, safety and security, and lifecycle software development. Software, was identified as the

primary theme in 83 of 124 articles. The secondary theme of Standards and Regulations was found in 36 of these 83 articles, while Risk Management accounted for 33 of the 83 articles as a secondary theme.

5.1.1. Functionality

The category Functionality incorporates the purpose of the SaMD, the features, the implementation and clinical use, as well as the various types that are currently available or in development. Once a device has been created with the intention of being SaMD, the safety and security of the device is only considered post-design. Importantly, these articles highlight the role of software assurance, safety, security, validation, and verification in SaMD. Additionally, this theme considered the role of SaMD functionality and purpose through the use and workflow of SaMD.

5.1.2. Safety and Security

The safety and security of the SaMD includes the privacy of data, and vulnerabilities impacting confidentiality, availability and integrity of the data, including software vulnerabilities. Safety of the user using the device is also considered as a factor within this category.

5.1.3. Software Development Lifecycle

Once standards and regulations incorporate SaMD into the software development lifecycle, manufacturers can ensure that the design and manufacturing of these device are compliant with standards.

5.2. Standards and Regulations

Once vulnerabilities and threats have been recognised, standards and regulations can be re-developed to include methods of addressing software vulnerabilities within the software development lifecycle. While standards and regulations were emphasized as a key theme in 30 of 124 of the articles, the articles relating to standards and regulation promoted frameworks that could regulate SaMD and discussed development of standards relating to SaMD.

5.3. Risk Management

Risk management can be used within the software development lifecycle to assess risks related to functionality, and to further assess risks related to the software deployment lifecycle itself. Risk management was discussed in 11 of the 124 articles, which emphasized the importance of regulations with regards to risk management.

Interestingly, 7 of the 11 risk management articles also discussed standards and regulations, and 9 of the 11 discussed software themes. Additionally, of the 30 articles that discussed standards and regulations, 7 also discussed risk management, while 21 of the 30, discussed software as a secondary theme.

Most significantly, the scoping review found that the three main themes were not mutually exclusive and that each article contained primary and secondary themes. Further analysis of the primary and secondary themes resulted in identification of common sub-themes consistent across the SaMD literature. The sub-themes identified were:

1. Principles, Concepts and Definitions
2. Standards
3. Classifications
4. Standards created by Organisations
5. Standards Implemented by member states
6. Lifecycle
7. Risk Management
8. Hazards
9. Consequences
10. Patient Safety
11. Research
12. Privacy
13. Security
14. Models and Frameworks
15. Validation and Verification of devices
16. Software assurance
17. Implementation and Clinical Use
18. IT and Clinical Personnel
19. Human Factors
20. Integrity
21. Purpose and Functionality
22. SaMD Types
23. Implantable
24. Health Apps
25. Medical devices with software
26. Wearable
27. Standalone

- 28. Wireless
- 29. Design and Development

These sub-themes were aggregated to the major themes as represented in Figure 1 and contribute to the understanding of SaMD components [2, 26-87]. Further analysis revealed what is currently missing from the SaMD components and. Interestingly, what is omitted from the literature is any comprehensive discussion of privacy. Hence, further research regarding the role of medical apps, and the impact on privacy is needed. The literature provides some indication of the boundaries of SaMD, and suggests that components such as privacy, software and IT system safety standards are highly important.

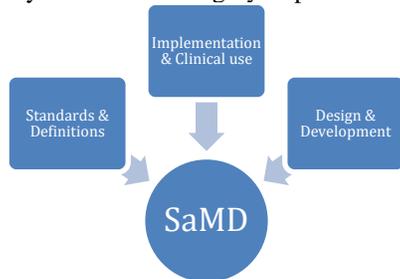


Figure 1. Components of SaMD taken from the literature [2, 26-87]

6. Discussion

6.1. SaMD Boundaries

Cobbaert [6] affirmed that identification of the intended use of SaMD can determine the boundaries of SaMD, and that a definition of these SaMD boundaries will result in a more concise definition which can be used to create standards. As explained by the literature, SaMD is complex, as there are several different contexts for SaMD use. The literature has demonstrated the multifaceted nature of SaMD and provides further justification to create standards that are suited for a rapidly evolving environment. Majchrowski [7] has explored both software and hardware contained in medical devices and has highlighted the importance of considering these aspects in the development of standards. Until now, the IMDRF has focused on the creation of a framework for regulating SaMD [8] which resulted in the creation of category types for devices based on public health impact. Hence, the IMDRF definition is a focused ‘regulator’ approach. This approach is not applicable to new innovative software and depending on the context, the definition may or may not be broad enough. Additionally, the IMDRF definition is not definitive and leads to interpretation, therefore,

leading to uncertainty in the marketplace. The International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO) through Joint WG7 have explored establishing guidelines, principles, common terms and definitions through the development of a road map for SaMD. This has specific relevance to the boundaries of SaMD as it will result in better categorisation. In addition, safety risk classification [3] of SaMD can result in greater product safety [2]. More importantly, one of the most critical shortcomings of the current SaMD definitions and standards are the lack of distinction between SaMD and medical apps. The next section explores how SaMD is used according to the literature.

6.2. How SaMD is Used

The role of SaMD and how it is used within the clinical environment is disparate, and has yet to be fully explored. There is currently confusion as to what SaMD specifically applies and where it should be applied. Ellis and Watson [9] report that electronic records should not be classified as medical devices as they are data collection tools; however, other authors [10] differ in this view as clinical support software (for instance health records, patient information and billing information) have been claimed to assist with the diagnosis and treatment of patients. Such an assessment leads to these tools being classified as SaMD based on the SaMD IMDRF definition. Highlighted in Figure 2 are the categories and uses of SaMD. They include categories such as Patient Centred, Provider Centred and General Clinical Software [12, 16, 21-85]. Additionally, the literature provides some indication of what SaMD is, but there is little information on SaMD components. Other categories of SaMD use have been identified, which include; stand-alone medical devices (active medical devices) [11], software add-ons and computer controlled devices [3]. There are a variety of uses for SaMD technologies, some of which include remote surgery, intelligent operating rooms [11] real time sensing, gait diagnosis [12], patient management software [13], as well as pacemakers, defibrillators and infusion pumps [14]. In particular, infusion pumps have been widely used for therapy and diagnosis of patients [15]. Other uses for SaMD include sensor management, disease prediction, microelectronic components and data and device integration [12]. While the literature has classified SaMD into three distinct categories, little research has been conducted into what role computer software, smart devices, medical apps [16, -17] and websites play in SaMD. Few studies have considered the wearable and implantable medical devices, wireless devices [14], Bluetooth

devices [12] and open versus proprietary clinical software [18] as SaMD. Therefore, further research into their role in patient safety and the benefits of SaMD is required.

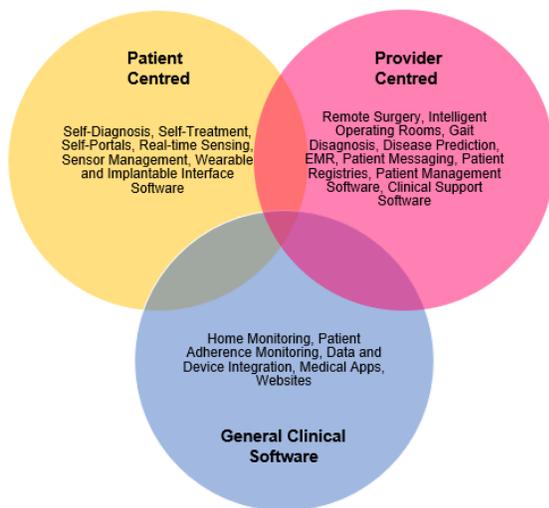


Figure 2. Categories to which the term SaMD has been applied [12, 16, 21-87]

The benefits of SaMD are well-recognised with a reported increase in expenditure (in 2015) and published worth of \$315 billion dollars globally [2]. While, 76% of SaMD deployment in 2015 was located in the USA, Japan, Italy and France, the USA has the largest market share with \$110 billion dollars spent in 2015, accounting for 35% of the global SaMD market [2]. Although SaMD represents significant benefits to patient safety, there is also a perceived and real risk when these technologies are compromised.

Interestingly, only three of the 124 articles discussed the need for regulation of medical apps. However, these articles discussed SaMD regulation, and suggested frameworks, based on inappropriate and broad definitions. Further, these articles do not discuss the boundaries of SaMD, nor do they attempt to define the boundaries. In addition, the fact that only three articles of 124 were found to include SaMD regulatory frameworks suggests that research is still needed on this topic. The analysis of themes also revealed the areas of SaMD that require additional research. For example, there was little published on information flow and SaMD. Although six of the 124 articles were found using the search term 'Software as Medical Device and information flow', it was found that these articles did not discuss how information flow is a factor in SaMD; therefore, further research into

information flow and SaMD is needed in order to understand all the aspects of SaMD.

Current risk management standards that look at software development, medical device manufacture and safety of health software, all rely upon traditional risk management as an essential part of the development process. This can be problematic as traditional risk management may not encompass modern SaMD. The optimum solution to this problem is the development of SaMD standards; this is however, not a simple and sequential process. Indeed, the complex and messy formulation of SaMD means that this is not a straightforward task when the boundaries of SaMD are not well defined. It was also found that the SaMD components are not sequentially linked and therefore a linear framework cannot provide a suitable solution. A suggested solution is for a framework that helps all stakeholders' (developers, clinicians, and patients) understanding of how SaMD can be practical, safe and useful, and one which describes the boundaries, components and relationships between components.

7. Outcome of the Scoping Review

The primary themes of SaMD from the literature (refer to Section 5) were further broken down into the components of SaMD. This analysis resulted in identification of SaMD categories of use

SaMD categories of use can be classified as: wireless applications, computer applications and medical applications. The identification of SaMD boundaries allows for the initial definition of SaMD itself.

One specific outcome of the study was that a revised definition of SaMD was needed and was developed, as current definitions did not suitably reflect the boundaries of SaMD. The revised definition was developed by identifying the purpose of SaMD and what its role as a device should ideally be. The main purpose of SaMD is medical management, with patient focus as the priority. Medical management refers to the treatment, monitoring, prevention and diagnosis of the patient. Following the identification of SaMD's role, the device architecture was then identified from the mapping of the boundaries. SaMD includes computer programs and other software such as mobile and wireless applications, which was included within the following initial definition.

7.1. Revised Definition

SaMD is standalone computer software programs or mobile applications that assist (treatment,

monitoring, prevention, diagnose) medical management of a patient e.g. Medical apps, clinical information systems.

8. Conclusion

A scoping review of the literature was conducted to identify the components and boundaries of SaMD. The purpose of this was to identify if a definition of SaMD could be described that articulated the boundaries of SaMD. The consensus view of the literature revealed that Risk Management, Standards and Regulations, and Software were all primary and secondary themes in the literature. As a primary theme, software was identified as including the sub-themes of software development lifecycle, safety and security of data, as well as functionality. The scoping review also revealed that SaMD has many categories of use, which include clinical support software, diagnosis tools, treatment and assessment tools, standalone medical devices, software-add-ons, computer-controlled devices, desktop systems, wearable and wireless technologies and much more. Additionally, the overall components of SaMD can be classified into principles, concepts and definitions, design and development as well as implementation and clinical use.

This research has concluded that there is no consensus view of what SaMD is, as the literature includes a broad scope that includes computer applications, wireless devices and medical apps. For example, the IMDRF define SaMD as “software intended to be used for one or more medical purposes that perform without being part of a hardware medical device” [5, p.6], while the European Commission’s Medical Devices Coordination Group has reclassified SaMD under their Medical Device Regulation (MDR). Additionally, many of the definitions of SaMD are contextually defined rather than properties based. Therefore, SaMD has no consistently defined boundaries as is highly contextual, and therefore could be considered an impractical term. This leads to uncertainty in the marketplace and carries an implication of the need for regulation to avoid the term. Future research needs to identify the properties of SaMD in order to define boundaries that can result in a definition that focuses on assuring patient safety when developing SaMD applications and using SaMD. The IMDRF definition of SaMD includes both high risk and low risk applications. Rather than use a context term such as SaMD, regulations should state what software is regulated; through use of clinical categories, such as EMR, patient registries, health records, etc. Currently, the term SaMD does not align with these clinical categories and results in ambiguity

in the marketplace, resulting in difficulty in interpretation for vendors of the regulations as they do not know if their software falls within the boundaries of SaMD. Regulators could look to use the IEC/ISO 82304-1 Standard [19] as a standards-based definition for SaMD, as this would allow both software developers and regulators to focus on enhanced clinical software safety. Further, international standards implementation may result in greater oversight for manufacturers of these devices with the potential to prevent patient harm as well as enhance privacy and security when using these devices.

9. Significance

This research has specifically drawn attention to the current lack of a consistent and consensus-based definition of SaMD. The challenges in defining the boundaries for SaMD and correlating these with the definitions have been highlighted and emphasises the need for this research. In addition, medical apps are an integral component of this context and their role in SaMD and medical device software failures needs to be addressed in order to suggest potential solutions through standards. Such standards can then be used to create frameworks to assure patient safety when using SaMD. This research will impact society by informing international standards development in this area as well as potentially the manufacturing practices of SaMD developers, to minimise information flow and interoperability issues that have the potential to lead to medical errors. Consequently, this will contribute to improved patient safety.

10. Ethical Considerations

No human ethical considerations were required as data collection was in the form of secondary research; therefore, the data collected was already published and does not pose any risks towards animals or people.

11. References

- [1] Mcpake, B., & Mahal, A. (2017). Addressing the Needs of an Aging Population in the Health System: The Australian Case. *Health Systems & Reform: Health Systems for Aging Societies in Asia and the Pacific*, Sponsored by the Nossal Institute for Global Health, The University of Melbourne, 3(3), 236-247.
- [2] Owono, G. F., Korrapati, R., Bush, R. & Stottlemeyer, D. (2015). *Impact of EU Medical Device Directive on Medical Device Software*, ProQuest Dissertations and Theses.
- [3] Simons, D. (1997). *Medical device software regulation: an industry perspective*. *Food and drug law journal*, 52(2), 189.

- [4] IEC (2010). Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities (IEC 80001-1). Geneva, Switzerland: ISO.
- [5] IMDRF. (2017). Software as a Medical Device (SaMD): Key Definitions: International Medical Device Regulators Forum (N41FINAL). IMDRF
- [6] Cobbaert, K. (2011). When does software become a medical device? *European Medical Device Technology*, 2(9), 21.
- [7] Majchrowski, B. (2009). Dialysis, Hazards, and Medical Device Software: Then and Now. *Biomedical Instrumentation & Technology*, 43(1), 59-62.
- [8] IMDRF (2014). "Software as a Medical Device": Possible Framework for Risk Categorization and Corresponding Considerations (N12FINAL). IMDRF.
- [9] Ellis, C. & Watson, E. (1999). Medical Device Software: Quality beyond Compliance, ProQuest Dissertations and Theses.
- [10] MDDI. (2012). Is your software a medical device? *European Medical Device Technology*, 3(2), 35.
- [11] Lee, I., Pappas, G. J., Cleaveland, R., Hatcliff, J., Krogh, B. H., Lee, P., & Sha, L. (2006). High-confidence medical device software and systems. *Computer*, 39(4), 33-38. doi: 10.1109/MC.2006.127
- [12] Wu, W. H., Bui, A. A. T., Batalin, M. A., Au, L. K., Binney, J. D., & Kaiser, W. J. (2008). MEDIC: Medical embedded device for individualized care. *Artificial Intelligence in Medicine*, 42(2), 137-152. doi: <http://dx.doi.org/10.1016/j.artmed.2007.11.006>
- [13] Agency, M. P. (2013). Medical Information Systems - Guidance for Qualification and Classification of Medical Information Systems. Sweden: Medical Products Agency.
- [14] MacKenzie, D. M. (1999). Designing safe software for medical devices. Paper presented at the, 1999. Proceedings of the 1999 International Conference on Software Engineering.
- [15] Ray, A., Jetley, R., & Jones, P. (2009). Engineering high confidence medical device software. *ACM DL*, 6(2), 1-7. doi: 10.1145/1859823.1859824
- [16] Muhamad, A. I., Rosman, M. R. M., Ramzi, M. I., & Salleh, M. I. M. (2012). Conceptualizing Medical Application Software for Managing Electronic Health Records (EHR) and Cash Flow Management in Private Clinics. *International Journal of Innovation, Management and Technology*, 3(2), 151. doi: <http://dx.doi.org/10.7763/IJIMT.2012.V3.213>
- [17] Hunt, W. A., Yauch, E. F., & Denovich, M. (1999). Computer software for processing medical billing record information: Google Patents.
- [18] Li, C., Raghunathan, A., & Jha, N. K. (2013). Improving the Trustworthiness of Medical Device Software with Formal Verification Methods. *IEEE Embedded Systems Letters*, 5(3), 50-53. doi: 10.1109/LES.2013.2276434
- [19] IEC/ISO 82304-1. (2016). Health software – Part 1: General requirements for product safety. Geneva, Switzerland: ISO.
- [20] Rostami, M., Bursleson, W., Juels, A., & Koushanfar, F. (2013). Balancing security and utility in Medical Devices? 2013 50th ACM/EDAC/IEEE Design Automation Conference (DAC), 1-6.
- [21] Kaufman, Michele B. (2011). Growth of mobile medical apps prompts FDA to seek input on proposed oversight approach. (App Watch: THE APPLICATION OF MOBILE MEDICAL APPS). *Formulary*, 46(8), 295-296.
- [22] Olusanya, O. (2013). Anaesthesia Exams by Medical Apps Ltd 2012. *Journal of the Intensive Care Society*, 14(2), 106.
- [23] Blanchet, K. (2012a). Medical Apps for Urologists. *BJU International*, 109(10), i-v. doi: 10.1111/j.1464-410X.2012.11213.x
- [24] MDDI. (2012). Is your software a medical device? *European Medical Device Technology*, 3(2), 35.
- [25] Wilson, H. (2006). Medical Devices Depend On Software. *Manufacturing Engineering*, 137(1), 59-60.
- [26] Fu, K., & Blum, J. (2014). Controlling for cybersecurity risks of medical device software. *Communications of the ACM*, 56(10), 35-37.
- [27] Lindholm, C., Notander, J., & Höst, P. (2014). A case study on software risk analysis and planning in medical device development. *Software Quality Journal*, 22(3), 469-497.
- [28] McCartney, M. (2013). How do we know whether medical apps work? *BMJ*, 346(mar20 1), f1811-f1811. doi: 10.1136/bmj.f1811
- [29] Fu, K. (2011). Trustworthy medical device software. Paper presented at the Institute of Medicine Workshop on Public Health Effectiveness of the FDA 510(k) Clearance Process.
- [30] Gagnon, L. (2014). Time to rein in the "Wild West" of medical apps. *CMAJ : Canadian Medical Association journal = journal de l'Association medicale canadienne*, 186(8), E247-E247. doi: 10.1503/cmaj.109-4772
- [31] Wicks, P., & Chiauzzi, E. (2015). 'Trust but verify'--five approaches to ensure safe medical apps. *BMC medicine*, 13(1), 205. doi: 10.1186/s12916-015-0451-z
- [32] Daw, Z., Cleaveland, R., & Vetter, M. (2014). Formal verification of software-based medical devices considering medical guidelines. *International Journal of Computer Assisted Radiology and Surgery*, 9(1), 145-153. doi: 10.1007/s11548-013-0919-2
- [33] Lincoln, J. E. (2012). Lifecycle Considerations for Device Software. *Journal of Validation Technology*, 18(1), 15-21.
- [34] Allen, S. (2014). Medical device software under the microscope. *Network Security*, 2014(2), 11. doi: 10.1016/S1353-4858(14)70021-2
- [35] Carroll, N. R. (2014). Mobile medical app regulation: preventing a pandemic of "mobilechondriacs". *Saint Louis University Journal of Health Law & Policy*, 7(2), 415.
- [36] Loughlin, S. (2016). In Contracts with Device Vendors, Mayo Clinic Emphasizes Security. *Biomedical Instrumentation & Technology*, 50(1), 53-53.
- [37] Barnes, D., Orbinati, Albert, & Greenberg, Alan. (2016). Cybersecurity and Medical Devices, ProQuest Dissertations and Theses.
- [38] Owens, B. (2016). Stronger rules needed for medical device cybersecurity. *The Lancet*, 387(10026), 1364-1364. doi: 10.1016/S0140-6736(16)30120-9
- [39] Yaman, H., Yavuz, E., Er, A., Vural, R., Albayrak, Y., Yardimci, A., & Asilkan, Ö. (2016). The use of mobile smart devices and medical apps in the family practice setting. *Journal of Evaluation in Clinical Practice*, 22(2), 290-296. doi: 10.1111/jep.12476
- [40] Liu, Y., Ren, W., Qiu, Y., Liu, J., Yin, P., & Ren, J. (2016). The Use of Mobile Phone and Medical Apps among General Practitioners in Hangzhou City, Eastern China. *JMIR*

- mHealth and uHealth, 4(2), e64. doi: <http://doi.org/10.2196/mhealth.4508>
- [41] Munn, Z., Peters, M., Stern, C., Tufanaru, C., McArthur, A., & Aromataris, E. (2018). Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. *BMC Medical Research Methodology*, 18(1), 143.
- [42] Bryman, A. (2016). *Social research methods* (Vol. 5th). Oxford;New York:: Oxford University Press.
- [43] Al Ayubi, S., Pelletier, A., Sunthara, G., Gujral, N., Mittal, V., & Bourgeois, F. C. (2016). A Mobile App Development Guideline for Hospital Settings: Maximizing the Use of and Minimizing the Security Risks of "Bring Your Own Devices" Policies. *JMIR mHealth and uHealth*, 4(2), e50. doi: <http://doi.org/10.2196/mhealth.4424>
- [44] Albrecht, U. (2013). Transparency of health-apps for trust and decision making. *J Med Internet Res*, 15(12), e277. doi: DOI: 10.2196/jmir.2981
- [45] Albrecht, U., & Von Jan, U. (2014). Medical apps in endocrine diseases – hide and seek. *Therapeutic Advances in Endocrinology and Metabolism*, 5(2), 23-33. doi: 10.1177/2042018814539375.
- [46] Alemzadeh, H., Iyer, R. K., Kalbarczyk, Z., & Raman, J. (2013). Analysis of Safety-Critical Computer Failures in Medical Devices. *IEEE Security & Privacy*, 11(4), 14-26. doi: 10.1109/MSP.2013.49
- [47] Alexandrou, A., Chen, Li-Chiou, Bear-Lehman, Jane, & Tao, Lixin. (2016). A Security Risk Perception Model for the Adoption of Mobile Devices in the Healthcare Industry, ProQuest Dissertations and Theses.
- [48] Ash, S., Riddell, Christopher M., & Burkhart, Bethany. (2016). Cybersecurity of Wireless Implantable Medical Devices, ProQuest Dissertations and Theses.
- [49] AHWP. (2014). White Paper on Medical Device Software Regulation – Software Qualification and Classification: AHWP.
- [50] Baker, S. D., Knudsen, J., & Ahmadi, D. M. (2013). The Wireless Challenge: Security and Safety For Medical Devices and Hospitals. *Biomedical Instrumentation & Technology*, 47(3), 208-208.
- [51] Bardy, G. H. (2001). System and method for automated collection and analysis of patient information retrieved from an implantable medical device for remote patient care: Google Patents.
- [52] Bearman, M., & Dawson, P. (2013). Qualitative synthesis and systematic review in health professions education. *Medical Education*, 47(3), 252-260. doi: 10.1111/medu.12092
- [53] Bierbrier, R., Lo, V., & Wu, R. C. (2014). Evaluation of the accuracy of smartphone medical calculation apps. *Journal of medical Internet research*, 16(2), e32. doi: DOI: 10.2196/jmir.3062
- [54] BJHC. (2006). Software to connect bedside medical devices. *The British Journal of Healthcare Computing & Information Management*, 23(4), 36.
- [55] Blanchet, K. (2012b). Medical Apps for Urologists: Usefulness still evolving for physicians and patients. *BJU International*, 109(10), i-v. doi: 10.1111/j.1464-410X.2012.11213.x
- [56] Bovee, M. W., Paul, D. L., & Nelson, K. M. (2001). A framework for assessing the use of third-party software quality assurance standards to meet FDA medical device software process control guideline's. *IEEE Transactions on Engineering Management*, 48(4), 465-478. doi: 10.1109/17.969424
- [57] Browne, G., O'Reilly, D., Waters, C., Tummon, O., Devitt, D., Stewart, B., & O'Connor, P. (2015). Smart-phone and medical app use amongst Irish medical students: a survey of use and attitudes. *BMC Proceedings*, 9(Suppl 1), A26. doi: <http://doi.org/10.1186/1753-6561-9-S1-A26>
- [58] Buijink, A. W. G., Visser, B. J., & Marshall, L. (2013). Medical apps for smartphones: lack of evidence undermines quality and safety. *Evid Based Med*, 18(3), 90. doi: 10.1136/eb-2012-100885
- [59] Carroll, N., & Richardson, I. (2016). Software-as-a-Medical Device: demystifying Connected Health regulations. *Journal of Systems and Information Technology*, 18(2), 186-215. doi: 10.1108/JSIT-07-2015-0061
- [60] Causey III, J. D., Purvis, R. E., & Henke, J. (2003). Handheld personal data assistant (PDA) with a medical device and method of using the same: Google Patents.
- [61] Cerkovnik, J., McDonald, Jeffrey T., Pardue, John H., Jacobs, Mike, & Yampolskiy, Mark. (2015). Managing Vulnerabilities and Risk in Networked Medical Devices, ProQuest Dissertations and Theses.
- [62] Commission, E. (2010). MEDICAL DEVICES: Guidance document GUIDELINES RELATING TO THE APPLICATION OF THE COUNCIL DIRECTIVE 93/42/EEC ON MEDICAL DEVICES DG Health and Consumer.
- [63] Communications, P. a. H. (2013). FDA medical app guidance regulates some apps, ignores others. *Pharmacy Times*, 79, 75.
- [64] Coward, J. (2010). Dental Patient Management Software Requires Medical Device Licence (pp. 22). Don Mills: Business Information Group.
- [65] Deora, S., & Dandekar, A. (2013). Quality, timeliness and reliability in software medical devices-experience.
- [66] El-Haiki, B., Mekki, K. S., & Ebrary. (2008). Medical device design for six sigma: a road map for safety and effectiveness (Vol. 2). Hoboken, N.J: Wiley-Interscience.
- [67] Ellouze, N., Allouche, M., Ahmed, H. B., Rekhis, S., & Boudriga, N. (2014). Security of implantable medical devices: limits, requirements, and proposals. *Security and Communication Networks*, 7(12), 2475-2491. doi: 10.1002/sec.939
- [68] Facchinetti, T., Fernando, A., & Quoi, R. (2012). This Process Is Just Beginning': Connecting Mobile Medical Devices. *Biomedical Instrumentation & Technology*, 46(2), 19-19.
- [69] Fan, J., Reparaz, O., Rozic, V., & Verbauwhe, I. (2013). Low-energy encryption for medical devices: Security adds an extra design dimension. Paper presented at the Design Automation Conference (DAC), 2013 50th ACM/EDAC/IEEE.
- [70] Fischmeister, S., & Azim, A. (2010). Design Choices for High-Confidence Distributed Real-Time Software (Vol. 6416, pp. 327-342). Berlin, Heidelberg: Springer Berlin Heidelberg.
- [71] Garg, A. X., Hackam, D., & Tonelli, M. (2008). Systematic Review and Meta-analysis: When One Study Is Just not

- Enough. *Clinical Journal of the American Society of Nephrology*, 3(1), 253-260. doi: 10.2215/cjn.01430307
- [72] Gehring, H., Pramann, O., Imhoff, M., & Albrecht, U. V. (2014). Zukunftstrend „Medical Apps: Vom App-Store direkt in die medizinische Anwendung? *Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz*, 57(12), 1402-1410. doi: 10.1007/s00103-014-2061-x
- [73] Goode, S. (2010). Exploring the supply of pirate software for mobile devices. *Information Management & Computer Security*, 18(4), 204-225. doi: <http://dx.doi.org/10.1108/09685221011079171>
- [74] Gopalakrishnan, S., & Ganeshkumar, P. (2013). Systematic Reviews and Meta-analysis: Understanding the Best Evidence in Primary Healthcare. *Journal of family medicine and primary care*, 2(1), 9.
- [75] Granger, A., Garrett, P., & Dalmadge, G. (2013). Medical device software risk assessment requires cross functional personnel. 2013 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 193-210.
- [76] Gupta, G. (2013). Are Medical Apps the future of medicine? *Medical journal, Armed Forces India*, 69(2), 105-106. doi: 10.1016/j.mjafi.2013.02.013
- [77] Hall, K. (2010). Developing medical device software to ISO 62304: medical software design standard ISO 62304 has just come into force. This article describes how it will impact the software development process for medical device manufacturers. *European Medical Device Technology*, 1, 22+.
- [78] Hei, X., Du, Xiaojiang, Lin, Shan, Bai, Li, & Wu, Jie. (2014). Security Issues and Defense Methods for Wireless Medical Devices, ProQuest Dissertations and Theses.
- [79] Höss, A., Lampe, C., Panse, R., Ackermann, B., Naumann, J., & Jäkel, O. (2014). First experiences with the implementation of the European standard EN 62304 on medical device software for the quality assurance of a radiotherapy unit. *Radiation oncology (London, England)*, 9(1), 79-79. doi: 10.1186/1748-717X-9-79
- [80] Huffman, A. (2015). With the Proliferation of Mobile Medical Apps, Which Ones Work Best in the Emergency Department? *Annals of Emergency Medicine*, 66(2), A13-A15. doi: 10.1016/j.annemergmed.2015.06.010
- [81] Hughes, G. (2012). Mobile device security (updated). *Journal of AHIMA / American Health Information Management Association*, 83(4), 50.
- [82] Huhn, M., & Zechner, A. (2010). Arguing for Software Quality in an IEC 62304 Compliant Development Process (Vol. 6416, pp. 296-311). Berlin, Heidelberg: Springer Berlin Heidelberg.
- [83] Jagannathan, S., & Sorini, A. (2016). Self-authentication in medical device software: An approach to include cybersecurity in legacy medical devices.
- [84] Jee, E., Lee, I., & Sokolsky, O. (2010). Assurance Cases in Model-Driven Development of the Pacemaker Software (Vol. 6416, pp. 343-356). Berlin, Heidelberg: Springer Berlin Heidelberg.
- [85] Jiang, Z., Abbas, H., Jang, K. J., & Mangharam, R. (2016). The Challenges of High-Confidence Medical Device Software. *Computer*, 49(1), 34-42. doi: 10.1109/MC.2016.20
- [86] Jones, R. D., Stalling, D. L., Davis, J., Jurkovich, P., & LaPointe, K. (2003). Software validation for medical device manufacturing. *The Quality Assurance Journal*, 7(4), 242-247. doi: 10.1002/qaj.245
- [87] Kabachinski, J. (2011). Mobile medical apps changing healthcare technology. *Biomedical instrumentation & technology / Association for the Advancement of Medical Instrumentation*, 45(6), 482.