Towards the Development of a Data Security Risk Management Framework for Medical Device Software AI Models

Buddhika Jayanethhthi[1[0009-0008-7813-3942]] Fergal Mc Caffery[1[0000-0002-0839-8362]] and Gilbert Regan[1[0000-0002-5023-6914]]

[1] Regulated Software Research Centre, Dundalk Institute of Technology, Dundalk, Ireland
buddhika.jayanethhthi@dkit.ie

Abstract. Data is considered the 'backbone' of the development of Artificial Intelligence (AI) models, including medical device software (MDS) AI models that process sensitive health data. Therefore, implementing necessary measures to assure data security is a key requirement that should be considered when developing MDS AI models. Developers face several challenges when assuring data security during the development of MDS AI models and the lack of guidance, i.e., a risk management standard or framework on managing the risks to sensitive health data is one of the major challenges they face. Moreover, the existing risk management standards and frameworks have several gaps and implementation challenges including: the lack of comprehensive threat and vulnerability lists; lack of a structured method for risk calculation or estimation; lack of a list of risk controls and risk control implementation details; and the need to refer to other standards and documentation for further information. Furthermore, current regulations and standards on AI model development recommend implementing a risk management process throughout the lifecycle of the AI model as a key requirement that should be employed for assuring data security. This paper presents the reasons behind the need for the development of a new developer friendly data security risk management framework that can be implemented by developers to assure data security when developing the MDS AI models. Additionally, this paper presents the elements that such a framework should contain. Ultimately, the framework should assist with improving the trustworthiness of AI and its adoption within the MDS industry and society.

Keywords: Artificial Intelligence, Data Security, Medical Device Software, Risk Management

1 Introduction

In recent years, Artificial Intelligence (AI) has shown a notable development [1]. AI has emerged as a promising tool for handling massive amounts of data to support complicated decision-making, a task that humans may find challenging or even impossible to do at times [2]. From 2017 to 2022, the global AI market has shown a compound annual growth rate (CAGR) of 18.3% [1]. Many industries, including healthcare,

manufacturing, engineering, education, and communication have been improved as a result of the advancements AI has brought to society. AI has the capability to revolutionise the healthcare domain and enhance the effectiveness and productivity of healthcare service delivery [3]. The Healthcare AI market is expected to grow at a CAGR of 38.1% between 2021 and 2030 [4]. The rise in volume and complexity of healthcare data is the primary driver of growth, making the integration of AI in healthcare essential [4]. Clinical decision-making that incorporates AI enhances patient outcomes and experience, optimises the operation of the health system, delivers value, lowers costs, and leverages the potential of big data [5].

Software is implemented in the medical device (MD) domain in two different ways: Software as a Medical Device (SaMD) and Software in a Medical Device (SiMD) [6]. The International Medical Device Regulators Forum (IMDRF) describes SaMD as software that is intended to be used for one or more medical purposes without necessarily being part of a hardware MD. Furthermore, it defines SiMD as software that is part of a hardware MD that helps the MD to achieve the intended medical purpose [6]. The majority of AL/ML-enabled MDs fall into the SaMD category [7]. An AI-enabled MD uses AI as a part or whole to achieve its intended medical purpose [8]. This paper uses the term 'Medical Device Software AI Models' to refer to the AI models embedded in MDS to perform their intended medical purposes.

As with other AI models, data is considered the 'backbone' of the development of MDS AI models and they usually rely on sensitive health data. Compromising this sensitive health data can lead to different issues including incorrect diagnosis, incorrect treatments, medical identity theft, and sometimes loss of patient life [9]. Hence, it is crucial to find effective ways to manage the risks to sensitive health data when developing the MDS AI models.

The goal of this paper is to present the need for the development of a new developer friendly data security risk management framework that can be used to assure data security when developing MDS AI models. This paper addresses the following objectives:

1. To identify the challenges that affect assuring data security when developing MDS AI models.
2. To identify the challenges for adopting a security risk management standard or framework.
3. To identify the gaps and implementation challenges of the existing risk management standards and frameworks.
4. To identify the data security requirements that should be fulfilled when developing MDS AI models.
5. To identify the elements that should be included in a developer friendly data security risk management framework for MDS AI models.

The paper is organised as follows, section 2 presents the findings of the literature review, section 3 presents the gaps and implementation challenges of the existing risk management standards and frameworks, section 4 presents the data security requirements that should be fulfilled when developing MDS AI models, section 5 presents the

structure of the proposed data security risk management framework, section 6 presents the future work and section 7 concludes the paper.

2 Literature Review

An extensive literature review was conducted to identify the data security challenges that affect the MDS AI model development and challenges that affect the adoption of a security risk management standard or framework. For the literature review a search was conducted on IEEE Xplore, ACM Digital Library, Science Direct (Elsevier) and Google Scholar using the search strings*; "Medical device software" AND (Artificial Intelligence OR AI) model development" AND "data security challenges" OR "data security issues" OR "data security risks" OR "data security problems" and "Security risk management" AND "(standard OR framework)" AND "(adoption OR implementation)" AND "(challenges OR barriers OR difficulties)"* respectively. The papers that meet the inclusion criteria of: (1) present data security challenges in MDS AI model development and challenges for adopting a security risk management standard or framework; (2) publication year: 2009-2024; (3) full-text available; (4) language: English; were considered for the review. In the first screening, each paper was reviewed by reading the abstract and conclusion and if the paper addressed any challenges, it was selected for the second screening. Otherwise, it was discarded. In the second screening, the full text of each paper was read to identify whether the paper presents any challenges for assuring data security of MDS AI models and challenges for adopting a security risk management standard or framework. Finally, a set of challenges presented in Section 2.1 and Section 2.2 were identified.

2.1 Data Security Challenges in MDS AI Model Development

Data is considered the 'backbone' of AI model development, including MDS AI model development that particularly relies on sensitive health data such as medication lists, diagnostic images and medical records of patients [10]. Compromising this sensitive health data can lead to several issues including incorrect diagnosis, incorrect treatments, medical identity theft, and sometimes loss of life [9]. Therefore, assuring data security is a key requirement that should be considered when developing MDS AI models. However, several challenges hinder the data security assurance of MDS AI models. The findings from the literature review have been published here [11], and this section presents a summary of the identified challenges.

Preventing Data Breaches. A data breach can expose sensitive patient health data to unauthorised parties which can lead to different issues including medical identity theft, privacy violations, incorrect diagnosis and treatment, and sometimes loss of patient lives [2, 9, 10]. The volume of healthcare data is increasing in complexity, variety, and timeliness, which raises the possibility of attacks [12]. It makes the application of security controls such as access controls, encryptions, data access monitoring and conducting regular security audits challenging [13]. Moreover, the evolving AI threat landscape challenges the implementation of security measures as the implementations

require more effort and new insights [14]. The existing security practices need to be accompanied by AI-specific practices which address the dynamic nature of the threats. For example, additional measures such as continuous risk management should be implemented throughout the entire lifecycle of the AI model [14].

Preventing Adversarial Attacks. An adversarial attack has the ability to change an AI model's input data, leading to inaccurate classifications in the model's output [15]. The two most prevalent adversarial attacks that affect MDS AI models are data poisoning and evasion [15]. MDS AI models usually process huge volumes of data making it impractical to check every single data point for possible poisoning. The detection requires efficient and scalable methods [13]. Additionally, both data poisoning and evasion attacks can be developed and transferred to different AI models, or versions of the same model, in order to maintain the model's vulnerability over time [16]. Hence, even if one defence measure mitigates a specific evasion or data poisoning approach, the attacker may find new methods to bypass the defence measures in future models [16]. Although defence measures such as adversarial training can be used to mitigate both data poisoning and evasion attacks, it is difficult to maintain a balance between accuracy, robustness and generalisation of the AI models [13, 16].

Preventing Cyberattacks. MDS AI models are significantly vulnerable to different cyberattacks such as hacking, spyware, ransomware and denial-of-service attacks [17]. The dynamic nature of cyberattacks makes it difficult to establish defense strategies as evolving cyberattacks cannot be prevented by static approaches like functional testing of predetermined behavior or static risk and failure rate calculation methods [18]. Even though encryptions and access controls can be used to prevent sensitive health data from cyberattacks, they have several limitations such as difficulty in using healthcare products and services, particularly in emergency conditions [17]. Although performing systematic software updates is essential to identify possible vulnerabilities, it has become a challenging task due to the high safety requirements of the MDs [19].

Preventing Insider Threats. Any malicious action conducted by an adversary who has previous knowledge and access to the MDS can compromise the data security of MDS AI models which necessitates robust access controls and methods to monitor user actions [20]. It is challenging to identify insider threats as they are skilled at bypassing mitigation measures without leaving anything suspicious [21]. Even though access controls can be used as a mitigation measure, striking a balance between access controls and providing seamless accessibility to healthcare services, especially in emergencies is a challenge. Limited access privileges can reduce accessibility [22].

Lack of Skilled and Trained Staff in AI and Data Security. One of the most prominent causes for healthcare data breaches are the lack of proper training of healthcare staff and users in avoiding data breaches and the lack of knowledge of mitigation measures [23]. Most of the MDS development organisations are small in size and usually lack staff with knowledge of existing security frameworks and guidelines and secure usage of AI [24]. Moreover, the healthcare service providing organisations that use the deployed MDS mainly focus on healthcare and usually lack experts in AI and data security [24]. Therefore, it may result in several problems, such as inadequate risk assessment and security planning, and inadequate security auditing processes [24]. Furthermore, the healthcare industry has difficulties in anticipating future security threats due to the lack of understanding of the need of assuring data security [25].

Lack of Guidance on Data Security Risk Management and Complexity of the Existing Risk Management Standards and Frameworks. Cruz and Tzavaras argue that it may be too early to integrate AI/ML into MD applications as the standards and regulations for AI/ML-enabled MD are still being developed [26]. It is still necessary to address the problem of lack of clarity related to the application of AI in the MD domain [27, 28]. In relation to the assurance of data security when developing MDS AI models, the most prominent challenge is the lack of a standard or framework that discusses data security risk management of MDS AI models [29]. Moreover, currently there are no standards or guidelines that address the risks associated with the use of adaptive algorithms in MDS AI models [26]. The National Institute of Standards and Technology has developed a risk management framework that provides guidelines for managing AI-related risks in AI systems [30]. However, it does not focus on the data security risk management of MDS AI models and does not provide any risk controls and respective implementation details for the controls [31]. The new AAMI 34971 standard does not address the data security risk management of MDS AI models; instead, it only provides directions on managing safety-related risks of AI/ML-enabled MDs [32]. Moreover, most of the existing standards and frameworks refer to other standards and documentation for further details which makes the implementation process more complicated and difficult than it needs to be [33, 34].

This study specifically focuses on addressing this challenge by developing a developer friendly data security risk management framework that can be conveniently used by the developers to assure data security when developing MDS AI models.

2.2 Challenges for Adopting a Security Risk Management Standard or Framework

Even though implementing a suitable security risk management standard or framework is considered one of the most effective ways of managing security risks, the adoption process requires overcoming several technical and organisational challenges and barriers [35]. This section presents the adoption challenges identified from the literature review.

Lack of Sufficient Details on the Implementation Process. Most of the existing standards and frameworks do not provide enough details that can be used by developers when implementing the standards and frameworks conveniently and efficiently [33, 36–39]. Hence, the lack of sufficient implementation details makes the implementation process complex and complicated.

Lack of Knowledge and Awareness of the Existing Standards and Frameworks. As the majority of MDS development organisations are small in size, they frequently lack knowledge and awareness of the security risk management frameworks and standards that are already in place [24, 40]. Typically, the developers working for those companies are inexperienced in choosing the best security risk management framework or standard for managing the risks of the MDS they develop [41, 42]. Therefore, they usually struggle to select the most suitable risk management standard/framework that should be applied to assure the data security of the MDS AI models they develop [41].

Selecting the Most Appropriate Standard or Framework for Implementation. The unavailability of a risk management standard or framework that specifically addresses data security risk management of MDS AI models or at least AI models in general makes the selection of a suitable standard or framework difficult and challenging [29]. The selection process is specifically a challenging task for the developers who lack knowledge of the available risk management standards or frameworks [43, 44]. Selecting the most applicable standard or framework requires a rigorous study of the existing risk management standards or frameworks which is a challenging task for inexperienced developers [45].

Lack of Risk Controls and Respective Implementation Details of the Risk Controls. In general, most of the existing risk management standards and frameworks do not provide the risk controls that can be used to mitigate the identified threats [33]. Additionally, they lack guidelines on how to implement the risk control measures [33, 46]. Hence, developers find the identification of suitable risk controls and the guidelines related to the implementation of the controls challenging when attempting to mitigate the identified threats [41, 43, 46].

Dynamic Data Security Threat Landscape. The evolving and complex data security threat landscape has also become a challenge for the adoption of a suitable risk management standard or framework [47, 48]. The existing risk management standards or frameworks do not provide guidance on how to react to the dynamically changing data security threats and implement necessary measures to prevent the evolving threats [49]. More specifically, the existing risk management standards and frameworks do not provide the necessary flexibility to address the data security risks that can occur in MDS AI models due to the use of adaptive algorithms [26].

Lack of Finance and Top Management Support. The top management personnel are usually resisting providing the required resources and support for the implementation of a risk management standard or framework due to the lack of knowledge of the return on investment [50, 51]. Most of them think it is a waste of money and time [33]. Moreover, the lack of sufficient budget allocated also makes the implementation process challenging [39].

3 Gaps and Implementation Challenges of the Existing Risk Management Standards and Frameworks

In addition to the literature review conducted to identify the data security challenges and risk management standard or framework adoption challenges, the existing risk management standards and frameworks in the domains of data or information security, AI, medical devices, and AI-enabled medical devices were evaluated to identify their gaps and implementation challenges. This section presents the criteria used to conduct the evaluation and the results obtained from the evaluation.

The criteria were developed by considering the adoption challenges identified in section 3, i.e., the lack of a risk management standard or framework that specifically discusses data security risk management of MDS AI models, the lack of sufficient implementation details, and lack of risk controls and risk control implementation details, and by

reviewing the current literature related to the risk management standards and frameworks evaluations and comparisons [33, 44, 46, 52–55]. The criteria were as follows:

1. Does the standard/framework provide guidelines for performing data security risk management of MDS AI models? [29]
2. Does the risk management standard/framework provide adequate steps for performing the risk management process? [52, 53] The adequate steps were identified based on the steps provided in the ISO 31000:2018 – Risk Management Guidelines, i.e., establishing the scope, context and criteria of the risk management process, risk assessment, risk treatment, monitoring and review, and recording and reporting.)
3. Does the standard/framework provide a comprehensive list of threats? [54]
4. Does the risk management standard/framework provide a comprehensive list of vulnerabilities? [53]
5. Does the risk management standard/framework detail a structured method for risk calculation/estimation (i.e., formulas, scale, matrix)? [53, 54]
6. Does the standard/framework provide risk controls? [54]
7. Does the standard/framework provide implementation details that can be followed to implement the risk controls? [33, 46, 55]
8. Does the standards/framework not recommend referring to other standards or supporting documentation for detailed information? [54]

To identify the existing risk management standards and frameworks, a search was conducted on the British Standard Institution (BSI) website and the Google search engine by the lead author and was overseen by members of the Regulated Software Research Centre (RSRC), DkIT, Ireland who have many years of experience in the domains of MDS development and risk management. Initially, a list of 206 standards/frameworks was collected, i.e., 176 from BSI and 30 from Google. During the first screening, revised/withdrawn/superseded and duplicate standards were removed which resulted in 112 standards/frameworks. Then during the second screening, the standards/frameworks were analysed by considering the full titles, scopes and descriptions of the 112 standards/frameworks to identify whether they discuss risks/managing risks in the considered domains. The second screening resulted in 18 standards/frameworks, i.e., 9 from BSI and 9 from Google. During the third screening, the 18 standards were examined in depth to identify whether they broadly discuss and present a risk management process that can be applied to managing risks in the considered domains. The third screening resulted in a list of 9 standards/frameworks.

The following 9 standards were included for evaluation: Two standards/frameworks from the data or information security domain, i.e., ISO/IEC 27005 [56] and NIST SP 800-39 [57]; three standards/frameworks from the AI domain, i.e., ISO/IEC 23894 [58], NIST 100-1 [30] and ENISA report on securing ML algorithms [59]; three standards from the medical device domain, i.e., ISO 14971 [60] and AAMI TIR 57 [61] and IEC/TR 80002-1 [62] and one standard from the AI-enabled medical device domain, i.e., AAMI TIR 34971[32] The summary of the results of the evaluation is presented in Table 1.

Table 1. Summary of the results of the evaluation.

	Criteria							
Standard/framework	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
ISO/IEC 27005	×	✓	✓	✓	✓	×	×	×
NIST SP 800-39	×	✓	×	×	×	×	×	×
ISO/IEC 23894	×	✓	×	×	×	×	×	×
NIST AI 100-1	×	✓	×	×	×	×	×	×
ENISA Report	×	×	✓	✓	×	✓	✓	×
ISO 14971	×	✓	×	×	×	✓	×	×
TIR 57	×	✓	✓	✓	×	✓	×	×
IEC/TR 80002-1	×	✓	×	×	×	✓	×	×
AAMI 34971	×	✓	×	×	×	✓	×	×

The following gaps and implementation challenges were identified from the evaluation:

- **Lack of a comprehensive list of threats and vulnerabilities:** only three standards/frameworks have provided lists of threats and vulnerabilities that can be used to understand the potential threats and vulnerabilities in the respective domains.
- **Lack of a structured method for risk calculation/estimation:** only one standard i.e., ISO/IEC 27005, has provided a structured method (qualitative risk matrix and a quantitative risk calculation scale) for risk calculation/estimation which is mandatory for identifying the risk levels associated with each threat and vulnerability combination.
- **Lack of a comprehensive list of risk controls and implementation details for the controls:** five standards have provided some possible examples of risks controls that can be used to mitigate the identified risks. However, none of them provide a detailed list of risk controls that can be used to mitigate each of the threats. Moreover, only one standard/framework i.e., the ENISA report, has provided risk control implementation details that can be used by the developers during implementation. Those implementation details were not comprehensive and did not outline the necessary steps that should be followed during the implementation of the risk controls (it has only provided some possible techniques).
- **Recommending to refer to other standards and documentation for further information:** all the standards/frameworks have recommended to refer to other standards and documentation for detailed information. It makes the implementation process complex and time consuming as the developers need to refer to several documents when implementing the risk management process.

The findings of the evaluation supported the adoption challenge identified in section 3. Moreover, the findings necessitated the development of a new comprehensive and

developer friendly data security risk management framework for assuring the security of sensitive health data when developing MDS AI models.

4 Data Security Requirements for MDS AI Model Development

Several regulations and standards from the EU and US markets were analysed to identify the data security requirements that should be fulfilled when developing MDS AI models. This section presents a summary of the identified data security requirements.

Five regulations: The EU AI Act [63]; the EU Medical Device Regulation (MDR) [64]; the General Data Protection Regulation (GDPR) [65]; the Health Insurance Portability and Accountability Act (HIPPA) [66] and WHO Guidance on Protection of Personal Data [67], three standards from the general AI domain: ISO/IEC 5338 [68]; ISO/IEC 8183 [69] and ISO/IEC 42001 [70] and two standards from the healthcare AI domain: BS 30440 [71] and ITU DEL2.2 [72] were included in the analysis. Even though the regulations and standards do not specifically mention the data security requirement that should be fulfilled when developing MDS AI models they have provided the following requirements that can be considered for assuring data security when developing MDS AI models.

- Implement a risk management process to identify and prevent data security threats throughout the development lifecycle of an AI model [64, 70–72].
- Implement suitable data security measures to mitigate data poisoning attacks [63, 68, 70], adversarial attacks [63], unauthorised access [63, 64, 66, 67, 72], disclosure [64, 66, 67], alterations, dissemination or loss of personal data [64].
- Perform risk assessment and risk treatment at regular intervals, planned intervals or when significant changes are needed [70].
- Implement measures such as encryption and pseudonymization to securely transmit and store personal information [64, 72].
- Establish a regular procedure to assess the efficacy of security measures and ensure continuous improvements [64, 67].
- Adhere to recommended cybersecurity procedures. A Data Protection Impact Assessment (DPAI) should be carried out at a minimum [71].
- Develop a list of risks connected to using the method of machine learning [72].

5 The proposed Risk Management Framework

To address the challenge of the lack of guidance for data security risk management when developing MDS AI models, the gaps and implementation challenges of the existing risk management standards and frameworks and to fulfill the data security requirement in the regulations and standards, this study proposes a new developer friendly data security risk management framework. The proposed framework will be developed based on the risk management process presented in the AAMI TIR 57 standard but will be incorporated with several enhancements compared to the risk management process provided in the AAMI TIR 57 standard, i.e., providing a comprehensive

list of threats and vulnerabilities, providing a structured method for risk calculation/estimation, a comprehensive list of risk controls and implementation details, a mapping of the threats, vulnerabilities, risk controls and implementation details to the phases of the AI model development lifecycle and steps to evaluate the overall residual risk acceptability.

The framework will comprise with following elements:

- A comprehensive list of data security threats and vulnerabilities to MDS AI models. Scientific papers, standards, technical reports, recent blog posts, websites and online databases will be used as sources to identify the threats and vulnerabilities.
- A structured method to calculate the risk associated with the identified threats and vulnerabilities. Qualitative, quantitative and semi-quantitative methods can be used for risk calculation [61]. The guidelines provided by NIST 800-30 and ISO/IEC 27005 will be used as sources to provide a structured method for risk calculation.
- A comprehensive list of risk controls and implementation details that can be used by the developers during the risk control implementation. Scientific papers, standards, technical reports, recent blog posts and websites will be used as sources to identify the risk controls and implementation details of the risk controls.
- A mapping of the threats, vulnerabilities, controls and implementation details to the phases of the AI model development lifecycle based on which phases the threats and vulnerabilities occur.
- AAMI TIR 57 states that there is a possibility of new risks being unintentionally added to the system due to the implementation of risk controls [61]. Hence, the proposed framework will provide a list of possible threats that can arise from the implementation of the proposed risk controls. Scientific papers, technical reports, blog posts, and websites will be reviewed for the identification process.
- Guidance for evaluating the overall residual risk acceptability. The framework will provide guidance for conducting penetration testing on AI models for evaluating the overall residual risk acceptability. Scientific research papers, technical reports, websites, and blog posts will be reviewed to develop the guidance.

6 Future Work

As part of the future work, the framework will be developed in three versions. The initial Alpha version will be developed by the lead author of the paper by including the elements stated in Section 5 and based on the risk management process presented in the AAMI TIR 57 standard. Upon completion of the development of the Alpha version, it will be validated using expert reviews collected from the experts in the domains of MDS AI model development or general AI model development, data security of AI models and risk management processes. The Alpha version will be upgraded to the Beta version by implementing the necessary suggestions and refinements identified during the expert review. Then the Beta version will be trialed in a medical device software development organisation that develops MDS AI models. The trial will conclude with an interview session to identify improvement suggestions and comments. Finally, the

Beta version will be upgraded to the Gama version by implementing the required refinements. Hence, eventually, the proposed framework will provide a data security risk management framework inclusive of all the sufficient implementation details that can be used by the developers to manage the risks to the security of sensitive health data during the development of MDS AI models in a convenient way.

7 Conclusion

Assuring data security is a key requirement that should be considered when developing MDS AI models. However, several challenges obstruct the data security assurance process and this study focuses on the fact that the lack of guidance, i.e., a risk management standard or framework for managing risks to sensitive health data when developing MDS AI models. Even though implementing a security risk management standard or framework is identified as one of the most effective and efficient ways to manage security risks, several challenges hinder the adoption process. With regards to managing the data security risks when developing MDS AI models, the lack of such data security standards or frameworks is a major challenge that the developers face. Moreover, the existing risk management standards and framework have several gaps and implementation challenges including the lack of a comprehensive list of threats and vulnerabilities, lack of a structured method for risk calculation or estimation, lack of risk controls and implementation details for the risk controls and referring to other standards and documentation for more details related to the risk management process which complicates the implementation. Hence, this study proposes a new developer friendly data security risk management framework for MDS AI models to address the identified challenges and fulfill the data security requirements detailed in the regulations and standards. The proposed framework will contribute to the MDS development industry by providing a well-structured and comprehensive data security risk management process and improving the trustworthy integration of AI in the MDS industry and society.

Acknowledgments. This study is financially supported by Ireland's Higher Education Authority (HEA) Technological University Transformation Fund (TUTF).

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Marketline: Global Artificial Intelligence Market Summary, Competitive Analysis and Forecast to 2027.
2. Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., Qadir, J.: Privacy-preserving Artificial Intelligence in healthcare: techniques and applications. Comput. in Biol. and Med. 158, 106848 (2023). https://doi.org/10.1016/j.compbiomed.2023.106848.
3. Spatharou, A., Heironimus, S., Jenkins, J.: Transforming healthcare with AI. (2020). https://doi.org/10.1002/9781119709183.ch3.

4. Allied Market Research: AI in healthcare market, https://www.alliedmarketresearch.com/artificial-intelligence-in-healthcare-market, last accessed 2023/08/15.
5. Chen, M., Decary, M.: Artificial Intelligence in healthcare: an essential guide for health leaders. Healthcare Manage. Forum. 33, 10–18 (2020). https://doi.org/10.1177/0840470419873123.
6. IMDRF SaMD Working Group: Software as a Medical Device (SaMD): key definitions. (2013).
7. FDA: Artificial Intelligence (AI) and Machine Learning (ML) in medical devices - executive summary for the patient engagement advisory committee meeting. (2020).
8. AIMD Working Group: Machine Learning-enabled Medical Devices : Key Terms and Definitions. (2022).
9. EPRS: Artificial Intelligence in healthcare: applications, risks, and ethical and societal impacts. (2022).
10. Coventry, L., Branley, D.: Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas. 113, 48–52 (2018). https://doi.org/10.1016/j.maturitas.2018.04.008.
11. Jayaneththi, B., McCaffery, F., Regan, G.: Data Security Challenges in AI-Enabled Medical Device Software. In: 2023 31st Irish Conference on Artificial Intelligence and Cognitive Science (AICS). pp. 1–6 (2023). https://doi.org/10.1109/AICS60730.2023.10470842.
12. Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., Saadi, M.: Big data security and privacy in healthcare: a Review. Procedia Comput Sci. 113, 73–80 (2017). https://doi.org/10.1016/j.procs.2017.08.292.
13. Dilmaghani, S., Brust, M.R., Danoy, G., Cassagnes, N., Pecero, J., Bouvry, P.: Privacy and security of big data in AI systems: a research and standards perspective. In: IEEE Int. Conf. on Big Data (Big Data). pp. 5737–5743. IEEE, Los Angeles, CA, USA (2019). https://doi.org/10.1109/BigData47090.2019.9006283.
14. ENISA: Multilayer framework for good cybersecurity practices for AI. (2023). https://doi.org/10.2824/588830.
15. Newaz, A.I., Haque, N.I., Sikder, A.K., Rahman, M.A., Uluagac, A.S.: Adversarial attacks to Machine Learning-based smart healthcare systems. In: IEEE Global Commun. Conf. (GLOBECOM 2020). , Taipei, Taiwan (2020). https://doi.org/10.1109/GLOBECOM42002.2020.9322472.
16. Gupta, K.D., Dasgupta, D.: Adversarial attacks and defenses for deployed AI models. IT Prof. 24, 37–41 (2022). https://doi.org/10.1109/MITP.2022.3180330.
17. Sarowa, S., Bhanot, B., Kumar, V., Kumar, M.: Analysis of attack patterns and cyber threats in healthcare sector. In: IEEE Int. Conf. on Device Intell. Comput. and Commun. Technol. (DICCT 2023). pp. 160–165. IEEE, Dehradun, India (2023).
18. Skierka, I.M.: The governance of safety and security risks in connected healthcare. In: Living in the Internet of Things: Cybersecurity of the IoT. pp. 1–12 (2018). https://doi.org/10.1049/cp.2018.0002.
19. Kwarteng, E., Cebe, M.: A survey on security issues in modern implantable devices: solutions and future issues. Smart Health. 25, 100295 (2022). https://doi.org/10.1016/j.smhl.2022.100295.
20. ENISA: AI cybersecurity challenges: threat landscape for Artificial Intelligence. (2020). https://doi.org/10.2824/238222.
21. Cheng, L., Liu, F., Yao, D.D.: Enterprise data breach: causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowl. Discovery. 7, (2017). https://doi.org/10.1002/widm.1211.

22. Janjua, F., Masood, A., Abbas, H., Rashid, I.: Handling insider threat through supervised machine learning techniques. Procedia Comput. Sci. 177, 64–71 (2020). https://doi.org/10.1016/j.procs.2020.10.012.
23. Seh, A.H., Zarour, M., Alenezi, M., Sarkar, A.K., Agrawal, A., Kumar, R., Khan, R.A.: Healthcare data breaches: insights and implications, (2020). https://doi.org/10.3390/healthcare8020133.
24. Chen, J.Q., Benusa, A.: HIPAA security compliance challenges: The case for small healthcare providers. Int. J. of Healthcare Manage. 10, 135–146 (2017). https://doi.org/10.1080/20479700.2016.1270875.
25. Holden, W.L.: Bridging the culture gap between healthcare IT and medical device development. Biomed. Instrum. and Technol. 48, 22–28 (2014). https://doi.org/10.2345/0899-8205-48.s2.22.
26. de la Cruz, R., Tzavaras, A.: AI Machine Learning and Medical Devices. BSI White Paper Series. (2024).
27. Grzybowski, A., Jin, K., Wu, H.: Challenges of artificial intelligence in medicine and dermatology. Clin Dermatol. (2024). https://doi.org/10.1016/j.clindermatol.2023.12.013.
28. Danese, C., Kale, A.U., Aslam, T., Lanzetta, P., Barratt, J., Chou, Y.B., Eldem, B., Eter, N., Gale, R., Korobelnik, J.F., Kozak, I., Li, X., Li, X., Loewenstein, A., Ruamviboonsuk, P., Sakamoto, T., Ting, D.S.W., Van Wijngaarden, P., Waldstein, S.M., Wong, D., Wu, L., Zapata, M.A., Zarranz-Ventura, J.: The impact of artificial intelligence on retinal disease management: Vision Academy retinal expert consensus. Curr Opin Ophthalmol. 34, 396–402 (2023). https://doi.org/10.1097/ICU.0000000000000980.
29. Zhao, H., Yang, G.: Information security and legal ethics of Artificial Intelligence medical devices, (2022).
30. NIST: Artificial Intelligence Risk Management NIST AI 100-1 Artificial Intelligence Risk Management. (2023).
31. Musser, M., Lohn, A.J., Dempsey, J.X., Spring, J.M., Kumar, R.S.S., Leong, B., Liaghati, C., Martinez, C., Grant, C.D., Rohrer, D., Frase, H., Elliott, J., Bansemer, J.D., Rodriguez, M., Regan, M., Chowdhury, R., Hermanek, S.: Adversarial Machine Learning and Cybersecurity: Risks, Challenges, and Legal Implications. ArXiv. abs/2305.1, (2023).
32. BSI: AAMI 34971: Application of BS EN ISO 14971 to machine learning in artificial intelligence – Guide, (2023).
33. Macmahon, S., Cooper, T., McCaffery, F.: Revising IEC 80001-1: risk management of health information technology systems. Comput. Standards & Interfaces. 60, 67–72 (2018). https://doi.org/https://doi.org/10.1016/j.csi.2018.04.013.
34. Paul, P.C., Loane, J., McCaffery, F., Regan, G.: Towards design and development of a data security and privacy risk management framework for WBAN based healthcare applications. Appl. Syst. Innov. 4, 704–710 (2021). https://doi.org/10.3390/asi4040076.
35. Townsend, K.: Organizations challenged with Cybersecurity Framework Implementation, https://www.securityweek.com/organizations-challenged-cybersecurity-framework-implementation/, last accessed 2023/10/14.
36. Eom, D., Lee, H.: A Holistic Approach to Exploring the Divided Standards Landscape in E-Health Research. IEEE Communications Standards Magazine. 2, 20–25 (2018). https://doi.org/10.1109/MCOMSTD.2018.1800007.
37. 37.Wang, X.R., Luo, W., Bai, X.L., Wang, Y.: Research on Big Data Security and Privacy Risk Governance. Proceedings - 2021 International Conference on Big Data, Artificial Intelligence and Risk Management, ICBAR 2021. 15–18 (2021). https://doi.org/10.1109/ICBAR55169.2021.00011.

38. Thapa, C., Camtepe, S.: Precision health data: Requirements, challenges and existing techniques for data security and privacy. Comput Biol Med. 129, 104130 (2021). https://doi.org/10.1016/j.compbiomed.2020.104130.
39. Benz, M., Chatterjee, D.: Calculated risk? A cybersecurity evaluation tool for SMEs. Bus Horiz. 63, 531–540 (2020). https://doi.org/10.1016/j.bushor.2020.03.010.
40. Alahmari, A., Duncan, B.: Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020. 10–14 (2020). https://doi.org/10.1109/CyberSA49311.2020.9139638.
41. Taylor, K., Smith, A., Zimmel, A., Alcantara, K., Wang, Y.: Medical Device Security Regulations and Assessment Case Studies. Proceedings - 2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems, MASS 2022. 742–747 (2022). https://doi.org/10.1109/MASS56207.2022.00116.
42. AlGhamdi, S., Win, K.T., Vlahu-Gjorgievska, E.: Information security governance challenges and critical success factors: Systematic review. Comput Secur. 99, 102030 (2020). https://doi.org/10.1016/j.cose.2020.102030.
43. Djebbar, F., Nordstrom, K.: A Comparative Analysis of Industrial Cybersecurity Standards. IEEE Access. 11, 85315–85332 (2023). https://doi.org/10.1109/ACCESS.2023.3303205.
44. Karie, N.M., Sahri, N.M., Yang, W., Valli, C., Kebande, V.R.: A Review of Security Standards and Frameworks for IoT-Based Smart Environments. IEEE Access. 9, 121975–121995 (2021). https://doi.org/10.1109/ACCESS.2021.3109886.
45. Granlund, T., Vedenpaa, J., Stirbu, V., Mikkonen, T.: On Medical Device Cybersecurity Compliance in EU. Proceedings - 2021 IEEE/ACM 3rd International Workshop on Software Engineering for Healthcare, SEH 2021. 20–23 (2021). https://doi.org/10.1109/SEH52539.2021.00011.
46. Yaqoob, T., Abbas, H., Atiquzzaman, M.: Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices-A Review. IEEE Communications Surveys and Tutorials. 21, 3723–3768 (2019). https://doi.org/10.1109/COMST.2019.2914094.
47. Siddiqui, F., Khan, R., Sezer, S.: Bird's-eye view on the Automotive Cybersecurity Landscape Challenges in adopting AI/ML. 2021 6th International Conference on Fog and Mobile Edge Computing, FMEC 2021. 1–6 (2021). https://doi.org/10.1109/FMEC54266.2021.9732568.
48. Fauzi, R., Sembiring, J.: A Review on Information Security Risk Assessment of Smart Systems : Risk Landscape , Challenges , and Prospective Methods. 2023 10th International Conference on ICT for Smart Society (ICISS). 1–6 (2023). https://doi.org/10.1109/ICISS59129.2023.10291306.
49. Naumov, S., Kabanov, I.: Dynamic framework for assessing cyber security risks in a changing environment. 2016 International Conference on Information Science and Communications Technologies, ICISCT 2016. 1–4 (2016). https://doi.org/10.1109/ICISCT.2016.7777406.
50. Han, L., Liu, J., Evans, R., Song, Y., Ma, J.: Factors Influencing the Adoption of Health Information Standards in Health Care Organizations: A Systematic Review Based on Best Fit Framework Synthesis. JMIR Med Inform. 8, e17334 (2020). https://doi.org/10.2196/17334.
51. Ključnikov, A., Mura, L., Sklenár, D.: Information security management in smes: Factors of success. Entrepreneurship and Sustainability Issues. 6, 2081–2094 (2019). https://doi.org/10.9770/jesi.2019.6.4(37).
52. Marks, L.: The optimal risk management framework. ISACA Journal. 1, 40–45 (2019).
53. ENISA: Compendium of risk management frameworks with potential interoperability. (2022). https://doi.org/10.2824/75906.
54. ENISA: Inteoperable EU Risk Management Framework - Methodology for assessment of interoperability among risk management frameworks and methodologies. (2022).

55. Mohammed, D., Mariani, R., Mohammed, S.: Cybersecurity challenges and compliance issues within the U.S. healthcare sector. Int. J. of Business and Social Res. 5, 55–66 (2015).
56. ISO/IEC: ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks. (2022).
57. NIST: NIST SP800-39 Managing Information Security Risk. (2011).
58. ISO/IEC: ISO/IEC 23894:2023 - Information technology — Artificial intelligence — Guidance on risk management. (2023).
59. ENISA: Securing Machine Learning Algorithms. (2021). https://doi.org/10.2824/874249.
60. ISO: ISO 14971 - Medical devices - Application of risk management to medical devices, International Standard. (2019).
61. AAMI: AAMI TIR 57: Principles for medical device security risk management. Association for the Advancement of Medical Instrumentation (AAMI) (2016).
62. ISO/IEC: IEC/TR 80002-1:2009 - Guidance on the application of ISO 14971 to medical device software. (2009). https://doi.org/10.2345/9781570203718.ch1.
63. European Commission: Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206, last accessed 2024/02/27.
64. European Commission: Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EE, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745, last accessed 2024/01/26. https://doi.org/10.1177/2165079915576935.
65. European Commission: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da.
66. HHS: Health Insurance Portability and Accountability Act of 1996 (HIPAA), https://www.hhs.gov/hipaa/for-professionals/index.html, last accessed 2024/01/27.
67. WHO: The protection of personal data in health information systems – principles and processes for public health. 35 (2020).
68. ISO/IEC: BS ISO/IEC 5338 Information technology — Artificial intelligence — AI system life cycle processes. (2022).
69. ISO/IEC: BS ISO / IEC 8183 : Information technology — Artificial intelligence — Data life cycle framework. (2023).
70. ISO/IEC: ISO/IEC 42001:2023-Information technology-Artificial Intelligence-management system. (2023).
71. BSI: BS 30440:2023-Validation framework for the use of artificial intelligence (AI) within healthcare - Specification. (2023).
72. ITU-T Focus Group on AI for Health: DEL2.2 Update: Good practices for health applications of machine learning: Considerations for manufacturers and regulators. (2022).