

An Evaluation of Risk Management Standards and Frameworks for Assuring Data Security of Medical Device Software AI Models

Buddhika Jayaneththi^a, Fergal Mc Caffery^b and Gilbert Regan^c
Regulated Software Research Centre, Dundalk Institute of Technology, Dundalk, Ireland

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

Abstract: Data is the backbone of Artificial Intelligence (AI) applications, including Medical Device Software (MDS) AI models which rely on sensitive health data. Assuring security of this sensitive health data is a key requirement for MDS AI models and there should be a structured way to manage the risk caused by data security compromises. Implementing a security risk management standard/framework is an effective way to develop a solid baseline for managing security risks, measuring the effectiveness of security controls and meeting compliance requirements. In this paper, nine risk management standards/frameworks in data/information security, AI, Medical Devices (MDs) and AI-enabled MDs domains are evaluated to identify their gaps and implementation challenges when applying them to assure data security of MDS AI models. The results show that currently there is no specific standard/framework that specifically addresses data security risk management of MDS AI models, and that existing standards/frameworks have several gaps such as complexity of the implementation process; lack of detailed threat and vulnerability catalogues; lack of a proper method for risk calculation/estimation; and lack of risk controls and control implementation details. These gaps necessitate the need for the development of a new data security risk management framework for MDS AI models.


1 INTRODUCTION


AI has the capability to revolutionise the healthcare sector and enhance the productivity and efficiency of care delivery (Spatharou et al., 2020). Integrating AI into clinical decision making helps reveal the power of big data, improve evidence-based decision making, deliver value by reducing cost, enhance patient experience and outcomes, and optimise health system performance (M. Chen & Decary, 2020). In the MD domain, software is implemented in two forms namely: Software in a Medical Device (SiMD) and Software as a Medical Device (SaMD) (IMDRF SaMD Working Group, 2013). The International Medical Device Regulators Forum (IMDRF) defines SaMD as software designed for one or more medical purposes without necessarily being part of a hardware MD. In contrast, SiMD is defined as a part of a hardware MD that assist the MD to perform the intended medical purpose (IMDRF SaMD Working Group, 2013).


Most devices that rely on AI/ML fall into the category of SaMD (FDA, 2020).

MDS AI models usually rely on sensitive personal health data including medical records, diagnostic images, and medication lists (Coventry & Branley, 2018). Exposure of this sensitive data to unauthorised parties can ultimately lead to different issues including medical identity theft, incorrect diagnosis and treatments, privacy and ethical violations, and sometimes life-threatening incidents or loss of lives (EPRS, 2022). Hence, assuring the security of this sensitive health data is a key requirement that should be considered when developing MDS AI models.

One of the most prominent issues that developers face when assuring data security when developing MDS AI models is the unavailability of a risk management standard/framework that specifically addresses the data security risk management of MDS AI models (Zhao & Yang, 2022). The development of such standard/framework requires the identification of the gaps and implementation challenges in the

^a  <https://orcid.org/0009-0008-7813-3942>

^b  <https://orcid.org/0000-0002-0839-8362>

^c  <https://orcid.org/0000-0002-5023-6914>

existing standards/frameworks. The contributions of this paper aim to fulfil the following objectives: 1) To identify the most relevant standards/frameworks that can be applied to the data security risk management of MDS AI models; 2) To evaluate the identified standards/frameworks, expose the state-of-art and identify the gaps and implementation challenges of the standards/frameworks and 3) To identify new requirements that should be fulfilled when developing a developer friendly data security risk management framework for MDS AI models .

As for the remaining parts of the paper, section 2 presents challenges faced when adopting a security standard/framework, section 3 presents the methodology used to conduct the evaluation, section 4 the results obtained, section 5 discussion, section 6 threats to validity and section 7 conclusion.

2 CHALLENGES FOR ADOPTING A SECURITY RISK MANAGEMENT STANDARD/Framework

This section presents a summary of the security risk management standard/framework adoption challenges identified from the literature.

Complexity and lack of sufficient implementation details: Most of the existing standards are complex and difficult to be understood and implemented by the developers as they do not provide enough implementation details (Eom & Lee, 2018; Macmahon et al., 2018).

Lack of awareness and knowledge of security standards/frameworks: Most of the organisations that develop MDS are usually small in size and often lack knowledge and awareness of existing data security standards and frameworks (J. Q. Chen & Benusa, 2017).

Selecting the most appropriate standard for implementation: The unavailability of a risk management standard/framework that specifically addresses data security risk management of MDS AI models makes the selection process challenging as it requires rigorous study of the existing ones (Djebbar & Nordstrom, 2023; Zhao & Yang, 2022).

Lack of security controls and control implementation details: In general, most of the standards/frameworks include security controls at a very high level with limited details related to the implementation of the security controls (Djebbar & Nordstrom, 2023; Macmahon et al., 2018; Yaqoob et al., 2019).

Lack of finance and top management support: Lack of top management support (Han et al., 2020) and limitations in the budget allocated (Benz & Chatterjee, 2020) also challenges the adoption process. Most of the top management personnel are reluctant to provide necessary resources and support due to the lack of understanding of the return on investment on application of the standard/framework (Macmahon et al., 2018).

Complex and dynamic data security threat landscape: Complex and evolving behaviour of the data security threat landscape is also challenging the adoption of an adequate security standard/framework (Siddiqui et al., 2021). The existing standards/frameworks are struggling to react to the dynamically changing security threat landscape and provide the necessary controls for the evolving threats (Naumov & Kabanov, 2016).

3 METHODOLOGY

The steps followed during the identification and evaluation of the standards and frameworks are depicted in Figure 1.

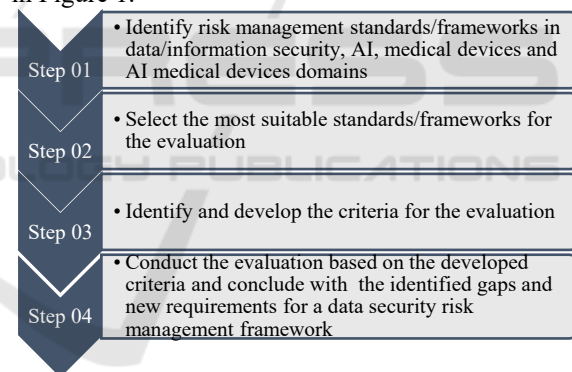


Figure 1: Methodology.

Step 01: To identify the existing risk management standards/frameworks, a search was conducted on the British Standard Institution (BSI) website and the Google search engine. The search was conducted by the lead author of the paper in October 2023, and was overseen by members of the Regulated Software Research centre (RSRC), DkIT, Ireland whom have many years of experience in the domain of MDS risk management. BSI provides access to British, European and International standards and the intention of using Google search was to identify any standards/frameworks that were not included in BSI. The search strings (SS) used to conduct the search are presented in Table 1.

Table 1: Search strings (SS) used.

	Search String
British Standard Institution	
1	“data security risk management”
2	“information security risk management”
3	“artificial intelligence risk management”
4	“artificial intelligence security risk management”
5	“medical device risk management”
6	“medical device security risk management”
7	“artificial intelligence medical device security risk management”
8	“artificial intelligence medical device software data security risk management”
Google	
9	“data security risk management standards and frameworks”
10	“information security risk management standards and frameworks”
11	“artificial intelligence risk management standards and frameworks”
12	“artificial intelligence security risk management standards and frameworks”
13	“medical device risk management standards and frameworks”
14	“medical device security risk management standards and frameworks”
15	“artificial intelligence medical device security risk management standards and frameworks”
16	“artificial intelligence medical device software data security risk management standards and frameworks”

An initial list of 176 standards was collected from the BSI. The list was filtered by removing the revised/withdrawn/superseded standards and duplicate standards in each SS. An initial list of 30 standards was collected from Google. During Google search, millions of records were derived for each SS. The first three pages of the search results were considered because Google’s page ranking system usually returns the highest quality and most relevant results for a user’s search query in the first pages. Any standard that was repeated from the BSI list was eliminated during the initial search. Then, the list was filtered by removing the duplicates collected for each SS. The summary of the collected standards is presented in Table 2.

Table 2: Summary of standards from the BSI.

SS	No: of standards	Revised/Withdrawn/superseded	Remaining
BSI			
1	100	27	73
2	78	20	58
3	2	1	1
4	0	0	0
5	47	16	31
6	15	2	13
7	0	0	0
8	0	0	0
Total			176
Duplicates of all search strings			85
Remaining Total			91
Google			
9	8	0	8
10	15	0	15
11	3	0	3
12	1	0	1
13	1	0	1
14	1	0	1
15	1	0	1
16	0	0	0
Total			30
Duplicates of all search strings			9
Remaining Total			21
Final Total from BSI and Google			112

Then an analysis was conducted by considering the full titles, scopes and descriptions of the 112 standards/frameworks to find whether they discuss risks/managing risks in the considered domains. During the analysis it was discovered that most of the standards that appeared in the initial list do not precisely discuss about risks/managing risks in the considered domains. For example: only 11 standards from SS 1 discuss risks/managing risks and all the 11 standards are repeated in the list of standards collected from SS 5. Hence, all the standards/frameworks that do not cover the risks/managing risks of considered domains were removed from the list. Based on the analysis, the initial list of standards was reduced to a secondary list of 18 standards/frameworks (9 from BSI and 9 from Google).

Step 02: The selected eighteen standards and frameworks were studied in depth to determine whether they broadly discuss a Risk Management Process (RMP) that can be applied to managing the risks in the considered domains. Based on this exercise, nine out of the eighteen standards and framework were selected for the evaluation. The rationale for the selection and elimination of the standards and frameworks is summarised in Table 3.

Table 3: Rationale for selection and elimination.

Standard/framework	Data/info Sec	AI RMP	MDR MP	AI MD RMP
Selected standards/frameworks				
ISO/IEC 27005:2022	✓	✗	✗	✗
NIST SP 800-39	✓	✗	✗	✗
BS ISO/IEC 23894:2023	✓	✓	✗	✗
NIST AI 100-1	✓	✓	✗	✗
ENISA report (Securing ML Algorithms)	✓	✓	✗	✗
ISO 14971	✗	✗	✓	✗
AAMI TIR57	✓	✗	✓	✗
IEC/TR 80002-1	✗	✗	✓	✗
BS/AAMI 34971	✗	✗	✗	✓
Eliminated standards/frameworks				
ISO/IEC 38507	✗	✗	✗	✗
NIST SP 800-37	✗	✗	✗	✗
ISO/IEC 27001	✗	✗	✗	✗
ISO/IEC 27557	✗	✗	✗	✗
ITSRM ² IT Security Risk Management Methodology V1.2	✓	✗	✗	✗
OCTAVE Allegro	✗	✗	✗	✗
OCTAVE FORTE	✗	✗	✗	✗
IEC 80001-1	✗	✗	✗	✗
MDCG 2019-16 Rev.1	✗	✗	✗	✗

Legend: ✓ - provide a RMP ✗ - does not provide a RMP

As detailed in Table 3, if the standard/framework provides a RMP in the considered domains it was included for the evaluation. The ITSRM² was eliminated as it provides the same RMP presented in ISO/IEC 27005: 2022 standard.

Step 03: The evaluation criteria were developed based on the existing literature related to risk management standards/frameworks evaluation (ENISA, 2022a, 2022b; Karie et al., 2021; Marks, 2019) and based on the identified adoption challenges detailed in section 2. The developed criteria for the evaluation are presented in Table 4.

Table 4: Criteria used for the evaluation.

Criteria	Criteria
1	Does the standard/framework address data security risk management of Medical Device Software AI models? (Zhao & Yang, 2022)
2	Does the standard/framework outline adequate phases of the risk management process? (ENISA, 2022a; Marks, 2019) Adequate stages of the RMP were identified based on the risk management process presented in ISO 31000:2018 – Risk Management Guidelines.
3	Does the risk management standard/framework provide threat catalogues? (ENISA, 2022b)

4	Does the risk management standard/framework provide vulnerability catalogues? (ENISA, 2022b)
5	Does the risk management standard/framework describe specific method for the calculation/estimation of risk (i.e. formulas, scale, matrix)? (ENISA, 2022b, 2022a)
6	Does the standard/framework provide risk controls? (ENISA, 2022b)
7	Does the standard/framework provide implementation details for the risk controls? (Macmahon et al., 2018; Mohammed et al., 2015; Yaqoob et al., 2019)
8	Does the standards/framework recommend referring to other supporting documentation for comprehensive/detailed information? (ENISA, 2022b)

Step 04: The nine standards/frameworks rigorously studied against the evaluation criteria to identify whether they meet the criteria or not. Based on the evaluation, gaps in the nine standards/frameworks, detailed in section 4 were identified. Furthermore, new requirements for a developer friendly data security risk management framework for MDS AI models detailed in section 7 were identified.

4 RESULTS

This section presents the results of the evaluation conducted on the nine selected standards.

4.1 Data/Information Security Risk Management

4.1.1 ISO/IEC 27005:2022 - Guidance on Managing Information Security Risks

This standard provides a RMP to conduct information security risk management for all types of organisations regardless of type, size or sector (ISO/IEC, 2022). The results of the evaluation are presented in Table 5.

Table 5: Results of ISO/IEC 27005 evaluation.

Criteria	Meets the criteria	Description
1	No.	It focuses on information security risks management in general.
2	Yes.	It uses the same RMP outlined in the ISO 31000:2018 standard.
3	Yes.	It provides a list of possible threats in Annex A (section A.2.5.1).
4	Yes.	It provides a list of vulnerabilities in Annex A (section A.2.5.2).
5	Yes.	Annex A provides a qualitative risk matrix and a quantitative risk calculation scale.

Table 5: Results of ISO/IEC 27005 evaluation (cont.).

Criteria	Meets the criteria	Description
6	No	It does not provide any risk controls. However, it recommends referring Annex A of ISO 27001 standard for risk controls.
7	No.	It does not provide implementation details for risk controls.
8	Yes.	It recommends referring ISO 27001 and ISO 31000 for more information

4.1.2 NIST SP 800-39 - Managing Information Security Risks

This standard provides guidance on how organisations can manage information security risks effectively within their operating environments (NIST, 2011). The results of the evaluation are presented in Table 6.

Table 6: Results of NIST SP 800-30 evaluation.

Criteria	Meets the criteria	Description
1	No	It focuses information security risks management in general.
2	Yes	It presents a RMP comprised of four core phases: framing/identifying risk, assessing risk, responding to risk and monitoring risk.
3	No	It only provides threat sources.
4	No	It does not provide any vulnerability catalogues.
5	No	It only states that risk is estimated by combining the likelihood that a threat will successfully exploit a vulnerability and result in an impact with severity of that impact.
6	No	It does not provide any risk controls.
7	No	It does not provide implementation details for risk controls.
8	Yes	It recommends referring NIST SP 800-37, NIST SP 800-53, NIST SP 800-53A and NIST SP 800-30.

4.2 AI Risk Management

4.2.1 ISO/IEC 23894:2023 - Information Technology - Artificial intelligence - Guidance on Risk Management

This standard outlines guidelines on how organisations that develop, deploy, or utilise products and services that employ AI can manage AI related risks (ISO/IEC, 2023). It assists organisations in integrating risk

management into their AI-related tasks and operations. The results of the evaluation are presented in Table 7.

Table 7: Results of ISO/IEC 23894 evaluation.

Criteria	Meets the criteria	Description
1	No	It focuses on AI-related risk management in general.
2	Yes	It uses the same RMP outlined in the ISO 31000:2018 standard.
3	No	It does not provide any threat catalogues.
4	No	It does not provide any vulnerability catalogues.
5	No	It only states that the organisations should assess the likelihood of occurrence of events and outcomes causing risks.
6	No	It does not provide any risk controls.
7	No	It does not provide implementation details for risk controls.
8	Yes	It recommends referring the ISO 31000 and ISO/IEC 22989:2022.

4.2.2 NIST AI 100-1 - Artificial Intelligence Risk Management Framework (AI RMF 1.0)

This framework provides guidance to organisations designing, developing, deploying or using AI systems on managing risks of AI and promoting trustworthy development and use of AI systems (NIST, 2023). The results of the evaluation are presented in Table 8.

Table 8: Results of NIST AI 100-1 evaluation.

Criteria	Meets the criteria	Meet/does not meet the criteria
1	No	It focuses on AI-related risk management in general.
2	Yes	The RMP outlined in the framework has four core stages: govern, map, measure and manage.
3	No	It does not provide any threat catalogues.
4	No	It does not provide any vulnerability catalogues.
5	No	It only states that the organisations may need to develop new types of risk measurements.
6	No	It does not provide any risk controls.
7	No	It does not provide implementation details for risk controls.
8	Yes	It recommends referring the NIST AI RMF Playbook.

4.2.3 ENISA Report – Securing Machine Learning Algorithms

This report identifies several cybersecurity threats that could target ML algorithms, potential vulnerabilities, security controls and some example techniques for operational implementation of the security controls (ENISA, 2021). The results of the evaluation are presented in Table 9.

Table 9: Results of ENISA report evaluation.

Criteria	Meets the criteria	Meet/does not meet the criteria
1	No	It focuses on risks related to ML algorithms in general AI/ML systems.
2	No	It does not provide steps to conduct risk management.
3	Yes	It provides six high-level cybersecurity threats and seven sub-threats.
4	Yes	It provides potential vulnerabilities associated with the identified threats.
5	No	It does not provide any guidelines for risk calculation/estimation.
6	Yes	It provides a list of security controls specific to attacks of ML algorithms and general attacks of AI systems.
7	Yes	It provides some example techniques for operational implementation of the security controls.
8	Yes	It suggests referring ISO 27001/2 and NIST 800-53

4.3 Medical Device Risk Management

4.3.1 ISO 14971 - Medical Devices: Application of Risk Management to Medical Devices

This standard presents guidance to develop a RMP for managing safety related risks of MDs, including Software as a Medical Device (SaMD) and in vitro diagnostic MDs (ISO, 2019). The results of the evaluation are presented in Table 10.

Table 10: Results of ISO 14971 evaluation.

Criteria	Meets the criteria	Description
1	No	It focuses on safety-related risks management of medical devices.
2	Yes	It outlines a RMP comprised of six core phases: risk analysis, risk evaluation, risk control, evaluation of overall residual risk, risk

		management review and production and post-production activities.
3	No	As it addresses safety-related risks, Annex C provides a list of potential hazards and foreseeable sequences of events that might produce hazardous situations and harm.
4	No	It does not provide any vulnerability catalogues
5	No	It only states that the risk estimation should be done by an analysis of the probability of occurrence of harm and the severity of the harm.
6	Yes	It provides some general risk control options.
7	No	It does not provide implementation details for risk controls.
8	Yes	It suggests referring ISO 24971 and ISO 13485.

4.3.2 AAMI TIR57 – Principles for Medical Device Security Risk Management

This standard presents guidance for MD manufacturers on methods that can be used to perform information security risk management for a MD based on the safety RMP proposed by ISO 14971 (AAMI, 2016). The results of the evaluation are presented in Table 11.

Table 11: Results of AAMI TIR 57 evaluation.

Criteria	Meets the criteria	Description
1	No	It focuses on information security risk management of MDs.
2	Yes	It provides the same phases outlined in the RMP of ISO 14971 standard.
3	Yes	It provides a list of possible threats in Annex B.
4	Yes	Annex B provides a list of vulnerability classes can be used as a starting point for the identification of vulnerabilities
5	No	It only states that the risk estimation should be done by combining the likelihood that a threat will successfully exploit a vulnerability and result in an impact with the severity of that impact.
6	Yes	It provides some general security risk control options. Annex E provides some practical examples of risk control measures with respect to a kidney system.
7	No	It does not provide implementation details for security risk controls.
8	Yes	It suggests referring NIST SP 800-30 and ISO 14971.

4.3.3 IEC/TR 80002-1:2009 - Guidance on the Application of ISO 14971 to Medical Device Software

This standard presents guidance on the application of the RMP outlined in *ISO 14971* to MDS with reference to *IEC 62304 - Medical device software - Software life cycle processes (ISO/IEC, 2009)*. The results of the evaluation are presented in Table 12.

Table 12: Results of IEC/TR 80002-1 evaluation.

Criteria	Meets the criteria	Description
1	No	It focuses on safety-related risk management of MDS.
2	Yes	It provides the same phases stated in the RMP of the ISO 14971 standard.
3	No	However, as it addresses safety-related risks, Annex A provides a list of hazards and foreseeable sequences of events that can produce hazardous situations and harm.
4	No	As the standard address safety-related risks, Annex B, Table B.1 provides a list of functional areas of software often related to hazards.
5	No	It only states that the risk estimation should be done by an analysis of the probability of occurrence of harm and the severity of the harm.
6	Yes	Annex B Table B.2 provides some possible risk control measures.
7	No	It does not provide implementation details for risk controls.
8	Yes	It suggests referring ISO 14971 and IEC 62304.

4.4 AI-Enabled Medical Device Risk Management

4.4.1 AAMI 34971:2023 - Application of BS EN ISO 14971 to Machine Learning in Artificial Intelligence-Guide

This standard provides guidance for applying ISO 14971 for performing safety risk management in AI/ML-enabled MDs (BSI, 2023). The results of the evaluation are presented in Table 13.

Table 13: Results of ISO 34971 evaluation.

Criteria	Meets the criteria	Description
1	No	It focuses on safety risk management of AI/ML enabled MDs

2	Yes	It provides the same steps stated in the ISO 14971 standard.
3	No	As it addresses safety-related risks, Annex B, Table B.1 gives examples of ML-related hazards.
4	No	It does not provide vulnerability list
5	No	It only states that the risk estimation should be done by an analysis of the probability of occurrence of harm and the severity of the harm.
6	Yes	It provides some ML risk controls.
7	No	It does not provide implementation details for security controls.
8	Yes	It suggests referring ISO 14971.

4.5 Summary of the Evaluation

A summary of the evaluation results is presented in the following Table 14.

Table 14: Summary of the evaluation.

Standard/ framework	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
	Criteria	1 ✗	✗	✗	✗	✗	✗	✗	✗
2	✓	✓	✓	✓	✗	✓	✓	✓	✓
3	✓	✗	✗	✗	✓	✗	✓	✗	✗
4	✓	✗	✗	✗	✓	✗	✓	✗	✗
5	✓	✗	✗	✗	✗	✗	✗	✗	✗
6	✗	✗	✗	✗	✓	✓	✓	✓	✓
7	✗	✗	✗	✗	✓	✗	✗	✗	✗
8	✓	✓	✓	✓	✓	✓	✓	✓	✓

Legend: ✓ - meet the criteria ✗ - does not meet the criteria

5 DISCUSSION

According to the results of the evaluation, it is evident that currently there is no standard/framework that specifically discusses data security risk management of MDS AI models and the existing ones have several gaps and implementation challenges.

Only three standards/frameworks provide threat and vulnerability catalogues that can be used to understand potential threats and vulnerabilities. This is a major gap as it is preferable to have knowledge of the existing threats and vulnerabilities to implement a RMP successfully.

Only one standard i.e., ISO/IEC 27005 provides a structured method (risk matrix/risk scale/formula) for the risk calculation/estimation of the risks. Risk

calculation/estimation is essential to identify the risk levels, severity of the risks and differentiate risks that should be mitigated and that can be accepted. Hence, it is identified as a primary gap in the existing standards/frameworks.

While five standards/frameworks provide some possible examples of risk controls that can be used to mitigate the identified threats and vulnerabilities, none of them provide a detailed list of risk controls that can be used during the implementation of the standards/frameworks. Identifying risks is not sufficient for a comprehensive RMP. It should provide methods/approaches for controlling the identified risks. Hence, this is identified as a major gap in the existing standards/frameworks.

Only one standard/framework i.e., ENISA report provides risk control implementation details that can be used by the developers to implement risk controls. However, these implementation details are not comprehensive and do not outline the necessary steps that should be followed during the implementation of the risk controls (it only provides some possible techniques). Hence, this is identified as a primary implementation challenge of existing standards/frameworks which makes the implementation process complicated and time consuming.

All standards/frameworks recommend referring to other standards or technical documentation for more details. This is a major gap in the existing standards/frameworks which makes the implementation process complex and time consuming. It necessitates the developers to read several documents to get a comprehensive understanding of the RMP provided in the standard/framework. Hence, the identified gaps and implementation challenges necessitate the development of a new comprehensive, straightforward and developer friendly data security risk management framework for MDS AI models.

6 THREATS TO VALIDITY

As the evaluation was done by a single researcher, there is a possibility for biases. The results may require validation by a panel of experts. Furthermore, there is a possibility for biases in the search conducted in Google due to the researcher's browsing history.

7 CONCLUSION

Assuring data security is a key concern that should be considered when developing MDS AI models and there should be a well-established and structured way

to manage the risk caused by data security compromises. Implementing a security risk management standard/framework is one of the most effective ways that is used to manage the risks effectively. However, standards/frameworks that specifically address data security risk management of MDS AI models do not exist. Existing risk management standards/frameworks have several gaps and implementation challenges which necessitates the development of a new developer friendly data security risk management framework for MDS AI models.

This paper identifies the need of the development of a new developer friendly data security risk management framework for MDS AI models. This evaluation was conducted as part of a PhD research which proposes to develop a new data security risk management framework for MDS AI models. The new framework should contain a comprehensive list of data security threats and vulnerabilities, a structured method for risk calculation/estimation, and a comprehensive list of security risk controls with respective implementation details. Moreover, the framework should be as all-inclusive as possible, with minimum references to other standards/documentations which makes the implementation process more complex and complicated than need be. The findings of this study can help researchers, developers, and other relevant stakeholders bring on further discussions on the development of new data security risk management standard/framework for MDS AI models and thus contribute to AI's trustworthiness and its adoption within MDS development industry and society.

ACKNOWLEDGEMENTS

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

REFERENCES

- AAMI. (2016). *AAMI TIR 57: Principles for medical device security risk management*. Association for the Advancement of Medical Instrumentation (AAMI).
- Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, 63(4), 531–540. <https://doi.org/10.1016/j.bushor.2020.03.010>
- BSI. (2023). *AAMI 34971: Application of BS EN ISO 14971 to machine learning in artificial intelligence – Guide*.
- Chen, J. Q., & Benusa, A. (2017). HIPAA security compliance challenges: The case for small healthcare

- providers. *Int. J. of Healthcare Manage.*, 10(2), 135–146. <https://doi.org/10.1080/20479700.2016.1270875>
- Chen, M., & Decary, M. (2020). Artificial Intelligence in healthcare: an essential guide for health leaders. *Healthcare Manage. Forum*, 33(1), 10–18. <https://doi.org/10.1177/0840470419873123>
- Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. *Maturitas*, 113, 48–52. <https://doi.org/10.1016/j.maturitas.2018.04.008>
- Djebbar, F., & Nordstrom, K. (2023). A Comparative Analysis of Industrial Cybersecurity Standards. *IEEE Access*, 11(July), 85315–85332. <https://doi.org/10.1109/ACCESS.2023.3303205>
- ENISA. (2021). *Securing Machine Learning Algorithms* (Issue December). <https://doi.org/10.2824/874249>
- ENISA. (2022a). *Compendium of risk management frameworks with potential interoperability* (Issue January). <https://doi.org/10.2824/75906>
- ENISA. (2022b). *Inteoperable EU Risk Management Framework - Methodology for assessment of interoperability among risk management frameworks and methodologies* (Issue January).
- Eom, D., & Lee, H. (2018). A Holistic Approach to Exploring the Divided Standards Landscape in E-Health Research. *IEEE Communications Standards Magazine*, 2(4), 20–25. <https://doi.org/10.1109/MCOMSTD.2018.1800007>
- EPRS. (2022). *Artificial Intelligence in healthcare: applications, risks, and ethical and societal impacts*.
- FDA. (2020). *Artificial Intelligence (AI) and Machine Learning (ML) in medical devices - executive summary for the patient engagement advisory committee meeting. ML*.
- Han, L., Liu, J., Evans, R., Song, Y., & Ma, J. (2020). Factors Influencing the Adoption of Health Information Standards in Health Care Organizations: A Systematic Review Based on Best Fit Framework Synthesis. *JMIR Medical Informatics*, 8(5), e17334. <https://doi.org/10.2196/17334>
- IMDRF SaMD Working Group. (2013). *Software as a Medical Device (SaMD): key definitions*.
- ISO. (2019). *ISO 14971 - Medical devices - Application of risk management to medical devices, International Standard* (Vol. 2000).
- ISO/IEC. (2009). *IEC/TR 80002-1:2009 - Guidance on the application of ISO 14971 to medical device software*. <https://doi.org/10.2345/9781570203718.ch1>
- ISO/IEC. (2022). *ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks*.
- ISO/IEC. (2023). *ISO/IEC 23894:2023 - Information technology — Artificial intelligence — Guidance on risk management*.
- Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access*, 9, 121975–121995. <https://doi.org/10.1109/ACCESS.2021.3109886>
- Macmahon, S., Cooper, T., & McCaffery, F. (2018). Revising IEC 80001-1: risk management of health information technology systems. *Comput. Standards & Interfaces*, 60(May), 67–72. <https://doi.org/https://doi.org/10.1016/j.csi.2018.04.013>
- Marks, L. (2019). The optimal risk management framework. *ISACA Journal*, 1, 40–45.
- Mohammed, D., Mariani, R., & Mohammed, S. (2015). Cybersecurity challenges and compliance issues within the U.S. healthcare sector. *Int. J. of Business and Social Res.*, 5(2), 55–66.
- Naumov, S., & Kabanov, I. (2016). Dynamic framework for assessing cyber security risks in a changing environment. *2016 International Conference on Information Science and Communications Technologies, ICISCT 2016*, 1–4. <https://doi.org/10.1109/ICISCT.2016.7777406>
- NIST. (2011). NIST SP800-39 Managing Information Security Risk. In *Nist Special Publication* (Issue March). <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>
- NIST. (2023). *Artificial Intelligence Risk Management NIST AI 100-1 Artificial Intelligence Risk Management*.
- Siddiqui, F., Khan, R., & Sezer, S. (2021). 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. <https://doi.org/10.1109/FMEC54266.2021.9732568>
- Spatharou, A., Heironimus, S., & Jenkins, J. (2020). Transforming healthcare with AI. In *Reimagining Businesses with AI* (Issue March). <https://doi.org/10.1002/9781119709183.ch3>
- Yaqoob, T., Abbas, H., & Atiquzzaman, M. (2019). Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices-A Review. *IEEE Communications Surveys and Tutorials*, 21(4), 3723–3768.
- Zhao, H., & Yang, G. (2022). Information security and legal ethics of Artificial Intelligence medical devices. *Forest Chemicals Review*, 236–245.