Data Security Challenges in AI-enabled Medical Device Software

Buddhika Jayaneththi
Regulated Software Research Centre
Dundalk Institute of Technology
Dundalk, Ireland
buddhika.jayaneththi@dkit.ie

Fergal McCaffery
Regulated Software Research Centre
Dundalk Institute of Technology
Dundalk, Ireland
fergal.mccaferry@dkit.ie

Gilbert Regan
Regulated Software Research Centre
Dundalk Institute of Technology
Dundalk, Ireland
gilbert.regan@dkit.ie

***Abstract*—The potential of AI to develop innovative applications that can benefit healthcare professionals and patients has created interest, especially in Medical Device Software (MDS) domain. However, the adoption of AI in MDS domain has created several challenges which include: making AI transparent; gaps in clarifying accountability; risk associated with the adaptive nature of AI algorithms; mitigating bias in data; lack of regulatory guidelines specific for AI; and assuring data security. Assuring data security is crucial for AI-enabled MDS, as compromising sensitive personal health data can create privacy and ethical concerns and sometimes lead to life threatening issues. In this paper, we discuss the importance of adopting AI in the healthcare domain, the importance of data security in AI-enabled MDS, and the data security challenges that AI has brought to the healthcare industry. Additionally, we consider the reasons for the existence of these challenges. The challenges discussed in this paper are in relation to (1) preventing data breaches; (2) preventing adversarial attacks; (3) preventing cyberattacks; (4) preventing insider threats; (5) lack of skilled and trained staff in data security; and (6) complexity of existing standards and lack of security control implementation details.**

Keywords—Artificial Intelligence, Healthcare, Medical Device Software

I. INTRODUCTION

There does not seem to be one generally agreed definition of Artificial Intelligence (AI). The United States Food and Drug Administration (FDA) define AI as the science and engineering of making intelligent machines, especially smart computer programs, using different techniques such as machine learning (ML), expert systems, and statistical data analysis models that basically depend on if-then logical conditions [1]. The European Commission defines AI as systems either entirely software-based or software embedded in special hardware devices that analyse their surroundings intelligently and take necessary actions to achieve specific goals [2]. Hence, in general, AI is about building smart machines or systems that can learn from experiences, adjust themselves to new processes and perform activities that generally need human intelligence.

AI has developed rapidly in recent years. Notably, AI has become a potential means for processing huge volumes of data to assist complex decision making, which may be difficult or sometimes impossible to be done by humans [3]. The global AI market has shown a compound annual growth rate (CAGR) of 50.3% between 2016 and 2021 [4]. The advances that AI has presented to society have improved a broad variety of industries including healthcare, manufacturing, engineering, education and communication. AI is unlocking new prospects in healthcare. It is now being utilised for a variety of research and healthcare functions including disease detection and quantification, healthcare service delivery, chronic condition management, drug discovery, and personalised treatments [5]. Besides the benefits that AI has brought to the healthcare industry, the adoption of AI has also brought various challenges including making AI transparent [6] , gaps in clarifying accountability [6]–[8], risk associated with the adaptive nature of AI algorithms [9], mitigating bias in data [7], lack of regulatory guidelines specific for AI [8] and assuring data security [7], [10]. With regards to data security, the healthcare industry utilises large volumes of sensitive patient data and compromising this sensitive data can create privacy and ethical concerns and sometimes lead to life threatening situations [6]. Hence, assuring the security of healthcare data is considered as a key concern of any medical device that handle sensitive patient data [6]. In this paper, we will discuss the importance of adopting AI in healthcare, the importance of assuring data security in AI-enabled MDS and the data security challenges that AI has bought to the healthcare industry in relation to the AI-enabled MDS. Additionally, we consider the reasons for the existence of these challenges.

II. THE ADOPTION OF AI IN HEALTHCARE

AI has the potential to revolutionise the healthcare industry and improve the productiveness and efficiency of care delivery [11]. Embedding AI into clinical decision making helps to unlock the power of big data, improve evidence-based decision making, deliver value and reduce cost, enhance patient experience and outcomes, and optimise health system performance [12]. AI in the healthcare market is projected to grow at a CAGR of 38.1% from 2021 to 2030 [13]. The growth is majorly driven by the increase in the volume and complexities of healthcare data which necessitates the integration of AI in healthcare [13].

In healthcare applications, AI-based systems are implemented as Software in a Medical Device (SiMD) or Software as a Medical Device (SaMD) [14]. 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 Medical Device (MD). In contrast, SiMD is defined as a part of a hardware Medical Device (MD) which assist the MD to perform the intended medical purpose [14]. In Europe, the Medical Device Regulations (MDR) uses the term MD to cover both SaMD and SiMD. This paper uses the term AI-enabled MDS to denote both SaMD and SiMD.

There are a few AI-enabled MDs approved and used in the USA and European markets. As of latest update on October 05, 2022, the Food and Drug Administration (FDA) has listed 521 approved AI-enabled MDs in the USA, out of which 91 devices have been approved in 2022 [15]. There is a notable growth in the number of approved devices in the USA from 2018 onwards which accounts for nearly 85% of all approved devices [16]. This remarkable increase could be linked to broader advancements of computing devices and software, availability of big data, cost effective cloud storage and investment from large companies [16]. In Europe, it is estimated that the Regulatory Bodies have approved 240 AI-enabled MDs, although this may be an underestimation as there is no publicly available database of all approved devices in Europe [17]. As the MD is considered safety critical, regulatory oversight of AI-enabled MD(S) is considered paramount [17]. Moreover, AI is considered an evolving and complex technology, and if AI is to be adequately integrated into the MDS industry then there is a vital need to assure, safety, efficacy and quality in order to gain public trust [17]. Assuring data security is one of the key challenges that needs to be addressed to gain that public trust.

III. DATA SECURITY AND AI-ENABLED MEDICAL DEVICE SOFTWARE

Data security is the process of protecting data from unauthorised access throughout its lifecycle, i.e., when the data is being gathered, processed, stored or transmitted, in order to preserve the confidentially, integrity and availability (CIA) of the data [18]. In the healthcare domain, data security is of utmost importance due to the sensitive nature of medical data and the potential consequences of security compromises. Exposure of medical data can eventually lead to medical identity theft, incorrect diagnosis and treatment [19]. Furthermore, impacts on personal health data can lead to privacy and ethical concerns and sometimes can cause life threatening incidents if contaminated data is used in treatment processes [6].

Data is often referred to as the "backbone" of any AI application including AI-enabled MDS. Data serves as the foundation on which AI algorithms and models are developed, trained and applied. AI-enabled MDS mainly rely on sensitive personal health data including medical records, diagnostic images, and personal health information [20]. The diversity of data sources, formats, data streaming techniques and infrastructure used in AI-enabled MDS may result in security vulnerabilities that can be exploited by adversaries [21]. Hence assuring data security of patient health records is a key requirement for AI-enabled MDS. Moreover, when considering security in the context of AI, the AI techniques and systems that use AI may be tampered with to manipulate the expected outcomes [22]. Thus, MDS developers should take necessary measures to assure the security of the data handled by the AI-enabled MDS. Before identifying and implementing the necessary protective measures, it is vital to identify the data security challenges precisely.

IV. DATA SECURITY CHALLENGES

The AI lifecycle of an AI-enabled MDS is composed of several phases which include: identifying the business problem; data collection; data exploration; data preprocessing; feature selection; model training; model tuning; model deployment and model maintenance [22]. Data security challenges can occur in different phases of the AI lifecycle. Fig. 1 developed by the lead author, shows a mapping of data security challenges to phases of the AI lifecycle.

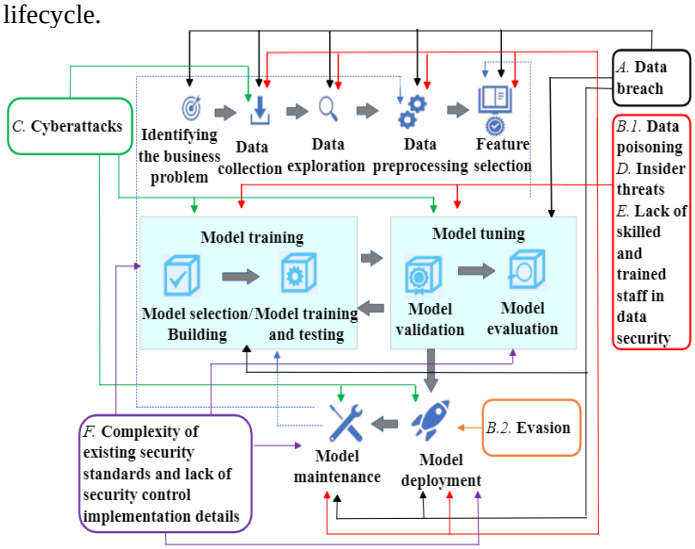

Figure 1:Mapping of challenges to AI lifecycle

A. *Preventing data breaches*

A data breach is a security violation or event that exposes sensitive and confidential data to an unauthorised party or results in its theft [10]. As a result of a data breach sensitive patient data could be exposed to unauthorised parties which might lead to identity theft, financial loss, loss of reputation, and reduced patient safety [3], [6], [20]. Moreover, healthcare data breaches may result in ethical issues such as privacy violations due to the confidential and sensitive nature of the data [23]. In AI-enabled MDS, a data breach can happen at almost every stage of the AI lifecycle [22]. In the AI-enabled MDS context, preventing data breaches has become a challenge due to the following reasons.

- *Complexity, diversity and volume of healthcare data*

The amount of healthcare data is growing in terms of complexity, diversity and timeliness [24]. Managing data across different platforms and stakeholders introduces complexity and increases the potential attack surface. The complexity and diversity of data make it challenging to implement effective controls such as access controls, encryption, regular security audits, monitoring data access, and de-identification [10].

- *Evolving threat landscape*

The threat landscape of AI systems is constantly evolving, with attackers introducing new techniques to breach AI systems. Rapidly evolving threats make it challenging to stay ahead of potential breaches as implementing security measures to defend against the evolving threats requires new insights and more effort [25].

- *Detecting internal data breaches*

Sometimes data breaches can also arise from insiders who have prior authorised access to the MDS [26]. Detection of internal data breaches is an extremely challenging task as the insiders may know how to bypass detection without leaving any suspicious evidence [26]. Hence, there should be strict monitoring processes implemented which requires more effort and cost [22].

B. Preventing adversarial attacks

During an adversarial attack, the adversary alters the input training data of an AI model to cause incorrect classification in the output and sometimes lead to shutdown of the entire application [27]. Preventing adversarial attacks is crucial for AI-enabled MDS as incorrect outputs generated by the AI models can negatively affect the safe and reliable performance of the MDS [27]. Data poisoning and evasion attacks are the most common types of adversarial attacks that affect AI-enabled MDS [27].

1. Data poisoning

Data poisoning is a type of adversarial attack in which an adversary intentionally manipulates the data of an AI model to manipulate the learned classifier by exploiting poor authentication/authorisation mechanisms [28]. In an AI-enabled MDS, data poisoning can occur in the data collection [22], [29], data exploration [22], data pre-processing [22], feature selection [22], model training [10], [22], [30] model tuning [22], model deployment especially when the AI model is adaptive and continuously learning from new operational data [22], and model maintenance [22] stages. Preventing data poisoning is a challenge due to the following reasons.

- *Scalability of data*

AI-enabled MDS often process large volumes of data, making it impractical to manually inspect every data point for potential poisoning. When the size of the dataset grows, identifying poisoned data instances becomes increasingly challenging, requiring efficient and scalable methods for detection [10].

- *Transferability of the poisoning attacks*

Data poisoning attacks can be designed to transfer across different models or versions of the same model. The transferability of poisoned data can be used by adversaries to keep AI models vulnerable, and it requires constant surveillance and defense procedures [31].

- *Limitations in the mitigation measures*

Adversarial training is one of the common defenses that can be used to mitigate data poisoning [32]. However, it has several limitations including, reducing the accuracy of the AI model, exposing the model to more generalisation and computational complexity [31], [32]. Hence, striking a balance between robustness, accuracy and generalisation is a challenge for developers. Moreover, these adversarial training techniques remain static and can be vulnerable to new attacks due to the evolving nature of the MDS threat landscape [31].

- *Stealthy nature of the attacks*

Data poisoning attacks are usually designed to be stealthy and difficult to detect. A small portion of poisoned data affects the entire dataset, causing detection of poisoned data more difficult. This makes it challenging to identify and differentiate between clean and poisoned data [27].

2. Evasion attack

An Evasion attack is a deliberate effort made by an adversary to manipulate input data of an AI model in a way that can mislead the model's predictions or classification outcomes generated at the deployment time [32]. The attacker tries to exploit vulnerabilities or weaknesses in the model's learning algorithm or feature space to make the model misclassify or provide a desired response. Evasion attacks affect the integrity of data and result in violation of user privacy [33]. In general, evasion happens in the deployment or application stage of the lifecycle, where the real-world data is applied to the trained model [10], [30]. Preventing evasion attacks is a challenge due to the following reasons:

- *Transferability of Evasion attacks*

As in data poisoning attacks, Evasion attacks can also be designed to transfer across different types of models or versions of the models. Even if a defense strategy defeats a particular evasion approach, the attacker may find ways to change their attack in later models to bypass the defense [31].

- *Limitations in the mitigation measures*

Although defense techniques such as adversarial training can be used to increase resilience against evasion attacks, it can impact how well the model generalises and performs with valid inputs. It is challenging to strike a balance between the robustness and generalisation of the model [10]. Moreover, adversarial training can compromise the accuracy of the AI model which can drastically affect safe performance of the MDS [32]. In general, adversarial training uses adversarial examples, i.e., data that have been deliberately modified to mislead the model, to train the model to be resistant to adversarial examples. The presence of adversarial examples in the training data set introduces a form of "noise" into the learning process. This noise can interfere with the model's ability to learn the true underlying patterns in the data, leading to a decrease in accuracy on clean data [34].

- *Handling computational overhead*

Many defense measures including adversarial training against evasion attacks involve additional computation steps that result in overhead and increase the computational requirements of the AI model [32]. Therefore, handling the computational overhead while mitigating evasion is a challenge for developers.

C. Preventing cyberattacks

The healthcare industry has suffered significantly from cyberattacks that compromise sensitive personal health data and professional information, costing millions of dollars in lost profits and fines [35]. AI-enabled MDS can be vulnerable to various cybersecurity attacks including hacking, spyware, ransomware, and denial-of-service attacks [36]. The interconnectivity and networking ability of MDS increases the attack vectors that can be exploited by cybercriminals [37]. In AI-enabled MDS, a cyberattack can usually happen in data collection, model training, model tuning, deployment [37] and maintenance [38] stages. Preventing cyberattacks is a struggle due to the following reasons:

- *Dynamic and evolving attacks*

Cyberattacks continue to evolve rapidly, and new attack techniques are constantly emerging. Keeping up with the latest threats and developing effective defenses is an ongoing challenge for developers [36]. Due to the dynamic and constantly evolving behavior of cyberattacks, security threats cannot be prevented by static and management methods such as functional testing of specified behavior and static risk and failure rate calculation techniques [39].

- *Assuring seamless accessibility of healthcare services*

Even though implementing robust encryption mechanisms and access control can prevent sensitive health data from cyberattacks, sometimes it can lead to difficulties in accessing healthcare services in emergency situations [36].

- *Conducting regular software updates*

Conducting regular software updates, which is necessary for identifying potential cyberattack vulnerabilities in MDS, is a challenge for the developers due to the strict safety requirements of MDs which use the MDS [40]. Any software update must undergo thorough testing to ensure that it does not introduce new bugs or security vulnerabilities that could compromise patient safety.

D. Preventing insider threats

An insider attack refers to any negative action that is performed by a malicious actor who has prior knowledge, access and authorisation to the system [26]. Insider threats can compromise data security, making it essential to implement strict access controls and monitor user activities [22]. Insider threats can significantly affect confidentiality and trustworthiness of a MDS [22]. In MDS domain, both the developers who develop the software [22] and the healthcare workforce [41] who use the deployed MDS can deliberately expose sensitive patient data. In AI-enabled MDS, an insider threat can happen during data collection, data exploration, data pre-processing, feature selection, model training, tuning, deployment and maintenance stages of the AI lifecycle [22]. Preventing insider threats has become challenge due to the following reasons:

- *Difficulties in detection*

In general, detecting insider threats tends to be a difficult task as their activities may not leave any evidence. Insiders have a good knowledge of the organisation, possibly having knowledge on how to bypass detection [42]. Moreover, with the aid of convert channels and steganography tools malicious insiders conduct data thefts usually difficult to detect [42]. Steganography tools typically provide the means to embed hidden data within various types of carrier files such as image files and videos [43]. For instance, in the MDS domain insiders can utilise image steganography to hide stolen sensitive patient data in a public cover image preventing indication of the presence of confidential and sensitive communication [43].

- *Diversity of the healthcare workforce*

In general, healthcare facilities have a diverse workforce, and not all staff members require access to all patient data. Even though role-based access controls can be used as a measure to reduce insider threats, limited access privileges can reduce the accessibility of healthcare services in emergency situations [41]. Hence, striking a balance between access controls and making necessary arrangements to provide better healthcare facilities, especially in emergency situations is a challenge for the healthcare service providers [41]. Moreover, implementing new trustworthy data access controls while adhering to appropriate security policies and schemes is a challenge due to the high diversity of the healthcare workforce [33]. Hence, the healthcare service providers should find ways to manage the access privileges with minimum effect to the emergency access of the MDS. Otherwise, it may affect the integrity of the services provided by the MDS and sometimes cause for life threatening incidents.

E. Lack of skilled and trained staff in data security

Public awareness of data security plays a vital role in assuring data security. The healthcare industry has been identified as one of the main industries which lacks knowledge on proper security defense and investment [44]. In terms of technical capabilities, the healthcare industry is behind other industries in securing healthcare data and infrastructure. Moreover, in terms of human capital, most healthcare providers do not have a leader solely responsible for data security [45]. Lack of skilled workforce in data security can affect data collection, data exploration, data pre-processing, feature selection, model training, tuning, deployment and maintenance stages of the AI lifecycle as data can be exposed to security risks at each of these stages.

- *Cybersecurity skill and resource shortage*

At present there is a remarkable cybersecurity skill gap and a shortage of resources [46]. The lack of knowledge on data security perspectives can lead to security threats as some healthcare staff who use the MDS may accidentally disclose sensitive patient data. A case study conducted to investigate security breaches that happened in several US based healthcare organisations has revealed that a lack of knowledge on protective measures such as encryption and lack of motivation for implementing protective measures from the leadership and development team are the prominent reasons for the healthcare data breaches [47]. Moreover, due to the lack of awareness of the importance of assuring data security, the healthcare sector faces a challenge in preparing for future security threats [48].

- *Scarcity of trained staff to implement cybersecurity frameworks*

Usually, organisations that develop MDS are small organisations with limited knowledge of data security frameworks and guidelines [49]. Consequentially, they often fail to develop relevant security policies to assuring data security [49]. Although IT security professionals can use cybersecurity frameworks to establish a reliable baseline for evaluating security performance and meeting compliance requirements, implementing these frameworks without the necessary resources, skills, and support from executive leadership is a challenge [50]. Moreover, small healthcare service providing organisations, who use the deployed MDS, primarily focus on healthcare and frequently lack expert IT knowledge. Hence it can lead to several issues including the lack of security planning and risk assessment, and lack of thorough security auditing procedures [49].

F. Complexity of existing security standards and lack of security control implementation details

There are several security standards and frameworks such as AAMI TIR57 – *Principles for Medical Device security – Risk management* [51] and pre-market [52] and post-market [53] guidelines proposed by the FDA that provide recommendations or best practices for assuring data security of MDs. However, the existing standards are complex to be understand by the developers [54] in that they tell you what to do but not how to do, and they do not provide adequate guidelines on how to implement the necessary controls to protect the data from security risks [54], [55]. For instance, the AAMI TIR57 [51] technical report provides details on what controls should be implemented to protect the data from security risks, but the report does not provide adequate guidelines on how to implement the necessary controls [54]. Moreover, AAMI TIR57 standard states that security risk controlling should be implemented during manufacturing,

deployment and monitoring stages of the MD [51]. Hence, when considering AI-enabled MDS, complexity and lack of security implementation details, can affect model training, tuning, deployment and maintenance stages of the AI lifecycle.

In general, The US and EU regulatory system is characterised by a certain degree of complexity, which also applies to cybersecurity regulations [56]. For example, [57] states that the IEC 80001-1 – *Application of risk management for IT-networks incorporating medical devices – Part 1* standard which addresses the risks associated with the incorporation of a medical device into an IT network, is too complicated and complex to implement. The organisations argue that the standard is too abstract and does not provide guidance on what steps need to be followed to implement the standard. Moreover, it was reported that the standard is depending on associated technical reports to provide guidance on the implementation of the standard and none of which provide the adequate details [57].

Moreover, there is a lack of security standards and frameworks that address security threats and controls related to AI-enabled MDS which is a significant challenge for developers [55]. Although the National Institute of Standards and Technology's (NIST) has taken efforts to develop an AI Risk Management Framework which includes some discussions on AI security, it remains unclear and does not discuss appropriate controls and control implementation details [58]. In addition, even though the recent AAMI TIR34971 - *Application of ISO 14971 to machine learning in artificial intelligence* [59] standard provides guidance on conducting safety risk management in AI or ML incorporating Medical Devices, it does not address data security risks and does not provide implementation guidelines on security control measures.

V. Conclusion

Assuring data security is considered as a key concern in AI-enabled MDS development. However, when assuring data security of AI-enabled MDS, developers face several challenges including preventing data breaches, preventing adversarial attacks, preventing cyberattacks, preventing insider threats, lack of skilled and trained staff in data security and complexity of existing security standards and lack of security control implementation details.

There are numerous reasons why each of these challenges exist, such as: Complexity, diversity and volume of healthcare data; Dynamic nature of the attacks; Insiders having knowledge on how to bypass detection; Cybersecurity skill shortage; and lack of adequate security standards in general, and in relation to AI.

For AI-enabled MDS to achieve its potential, it must be trusted, and data security is a pre-requisite. Hence, developers and researchers need to address the above mentioned reasons in order to mitigate the challenges. The contributions of this paper can be used as a basis for development of the necessary measures to address the reasons behind the challenges, and thus contribute the trustworthiness of AI enabled MDS and its adoption within society.

Acknowledgment

This work is financially supported by the Higher Education Authority (HEA) Technological University Transformation Fund (TUTF).

References

[1] FDA, "Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan," 2021.

[2] European Commission, "A definition of Artificial Intelligence: main capabilities and scientific disciplines," Brussels, Apr. 2019. Accessed: Mar. 20, 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

[3] N. Khalid, A. Qayyum, M. Bilal, A. Al-Fuqaha, and J. Qadir, "Privacy-preserving artificial intelligence in healthcare: Techniques and applications," *Comput Biol Med*, vol. 158, no. March, p. 106848, 2023

[4] Marketline, "Global Artificial Intelligence Market Summary, Competitive Analysis and Forecast, 2017-2026," *Marketline*, 2022. https://store.marketline.com/report/global-overview-of-artificial-intelligence-market-and-analysis/#product-1387434 (accessed Jul. 18, 2023).

[5] FDA, "Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)," 2019. Accessed: Mar. 28, 2023.[Online].Available:https://www.fda.gov/files/medical%20devices/published/US-FDA-Artificial-Intelligence-and-Machine-Learning-Discussion-Paper.pdf

[6] EPRS, "Artificial intelligence in healthcare: applications, risks, and ethical and societal impacts.," 2022.

[7] A. Ndrejaj and M. Ali, "Artificial Intelligence Governance: A Study on the Ethical and Security Issues that Arise," *Proceedings - 2022 International Conference on Computing, Electronics and Communications Engineering. iCCECE 2022*, pp. 104–111, 2022

[8] N. Hrgarek, "Certification and regulatory challenges in medical device software development," in *2012 4th International Workshop on Software Engineering in Health Care, SEHC 2012 - Proceedings*, 2012, pp. 40–43. doi: 10.1109/SEHC.2012.6227011.

[9] M. Hayes and Curran, "AI in Medical Devices: Key Challenges and Global Responses," *Mason Hayes and Curran*, 2021, [Online]. Available: https://www.mhc.ie/latest/insights/ai-in-medical-devices-key-challenges-and-global-responses

[10] S. Dilmaghani, M. R. Brust, G. Danoy, N. Cassagnes, J. Pecero, and P. Bouvry, "Privacy and Security of Big Data in AI Systems: A Research and Standards Perspective," in *2019 IEEE International Conference on Big Data (Big Data)*, IEEE, Dec. 2019, pp. 5737–5743. doi: 10.1109/BigData47090.2019.9006283.

[11] A. Spatharou, S. Heironimus, and J. Jenkins, "Transforming Healthcare with AI," 2020. doi: 10.1002/9781119709183.ch3.

[12] M. Chen and M. Decary, "Artificial intelligence in healthcare : An essential guide for health leaders," *Helathcare Management Forum*, vol. 33, no. 1, pp. 10–18, 2020, doi: 10.1177/0840470419873123.

[13] Allied Market Research, "AI in Healthcare Market," *Allied Market Research*, 2021. https://www.alliedmarketresearch.com/artificial-intelligence-in-healthcare-market (accessed Aug. 15, 2023).

[14] IMDRF, "IMDRF/SaMD WG/N10FINAL:2013 Final Document Title: Software as a Medical Device (SaMD): Key Definitions," 2013.

[15] FDA, "Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices," *www.fda.gov*, 2022. https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-aiml-enabled-medical-devices (accessed Aug. 25, 2023).

[16] G. Joshi, A. Jain, S. Adhikari, H. Garg, and M. Bhandari, "FDA approved Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices: An updated 2022 landscape," *medRxiv*, p. 2022.12.07.22283216, Jan. 2023

[17] U. J. Muehlematter, P. Daniore, and K. N. Vokinger, "Approval of artificial intelligence and machine learning- based medical devices in the USA and Europe (2015 – 20): a comparative analysis," *Lancet Digit Health*, vol. 3, no. 3, pp. 195–203, 2021.

[18] Y. He and C. W. Johnson, "Generic security cases for information system security in healthcare systems," *IET Conference Publications*, vol. 2012, no. 607 CP, pp. 1–6, 2012

[19] S. Chandra, S. Ray, and R. T. Goswami, "Big Data Security in Healthcare Survey on Frameworks and Algorithms," *2017 IEEE 7th International Advance Computing Conference (IACC)*, pp. 89–94, 2017, doi: 10.1109/IACC.2017.0033.

[20] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, no. April, pp. 48–52, 2018

[21] D. S. Terzi, R. Terzi, and S. Sagiroglu, "A survey on security and privacy issues in big data," *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, pp. 202–207, 2016, doi: 10.1109/ICITST.2015.7412089.

[22] ENISA, "AI Cybersecurity Challenges-Threat Landscape for Artificial Intelligence," Dec. 2020. doi: 10.2824/238222.

[23] A. O. Ugwu, X. Gao, J. O. Ugwu, and V. Chang, "Ethical Implications of AI in Healthcare Data: A Case Study Using Healthcare Data Breaches from the US Department of Health and Human Services Breach Portal between 2009-2021," *Proceedings - 2022 International Conference on Industrial IoT, Big Data and Supply Chain, IIoTBDSC 2022*, pp. 343–349, 2022, doi: 10.1109/IIoTBDSC57192.2022.00070.

[24] H. K. Patil and R. Seshadri, "Big data security and privacy issues in healthcare," *Proceedings - 2014 IEEE International Congress on Big Data, BigData Congress 2014*, pp. 762–765, 2014

[25] N. Polemi and I. Praça, "Multilayer framework for Good Cybersecurity Practices for AI," 2023. doi: 10.2824/588830.

[26] W. Hurst, B. Tekinerdogan, T. Alskaif, A. Boddy, and N. Shone, "Securing electronic health records against insider-threats: A supervised machine learning approach," *Smart Health*, vol. 26, no. April, 2022, doi: 10.1016/j.smhl.2022.100354.

[27] A. I. Newaz, N. I. Haque, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "Adversarial Attacks to Machine Learning-Based Smart Healthcare Systems," *2020 IEEE Global Communications Conference, GLOBECOM 2020 - Proceedings*, 2020

[28] N. Baracaldo, B. Chen, H. Ludwig, and J. A. Safavi, "Mitigating poisoning attacks on machine learning models: A data provenance based approach," *AISec 2017 - Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security, co-located with CCS 2017*, pp. 103–110, 2017, doi: 10.1145/3128572.3140450.

[29] OWASP, "OWASP AI Security and Privacy Guide," *https://owasp.org/www-project-ai-security-and-privacy-guide/*, Feb. 15, 2023. https://owasp.org/www-project-ai-security-and-privacy-guide/ (accessed Jun. 07, 2023).

[30] Y. Hu *et al.*, "Artificial Intelligence Security : Threats and Countermeasures," *ACM Comput Surv*, vol. 55, no. 1, 2021.

[31] K. D. Gupta and D. Dasgupta, "Adversarial Attacks and Defenses for Deployed AI Models," *IT Prof*, vol. 24, no. 4, pp. 37–41, 2022

[32] A. Oprea and A. Vassilev, "Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations," 2023, [Online].Available: https://csrc.nist.gov/publications/detail/white-paper/2023/03/08/adversarial-machine-learning-taxonomy-and-terminology/draft

[33] S. Venkatraman and R. Venkatraman, "Big data security challenges and strategies," *AIMS Mathematics*, vol. 4, no. 3, pp. 860–879, 2019, doi: 10.3934/math.2019.3.860.

[34] H. Wang, T. Chen, S. Gui, T. K. Hu, J. Liu, and Z. Wang, "Once-for-all adversarial training: In-situ tradeoff between robustness and accuracy for free," *Adv Neural Inf Process Syst*, vol. 2020-Decem, no. NeurIPS, 2020.

[35] M. Paul, L. Maglaras, M. A. Ferrag, and I. Almomani, "Digitization of healthcare sector: A study on privacy and security concerns," *ICT Express*, no. xxxx, 2023

[36] S. Sarowa, B. Bhanot, V. Kumar, and M. Kumar, "Analysis of Attack Patterns and Cyber Threats in Healthcare Sector," *Proceedings - IEEE International Conference on Device Intelligence, Computing and Communication Technologies, DICCT 2023*, pp. 160–165, 2023

[37] A. Alsuwaidi, A. Hassan, F. Alkhatri, H. Ali, M. Qbeaah, and S. Alrabaee, "Security Vulnerabilities Detected in Medical Devices," *Proceedings - 2020 12th Annual Undergraduate Research Conference on Applied Computing, URC 2020*, 2020

[38] M. Aijaz, M. Nazir, and M. N. Anwar, "Classification of Security Attacks in Healthcare and associated Cyber-harms," *Proceedings of the 1st International Conference on Advances in Computing and Future Communication Technologies, ICACFCT 2021*, pp. 166–173, 2021, doi: 10.1109/ICACFCT53978.2021.9837349.

[39] I. M. Skierka, "The governance of safety and security risks in connected healthcare," *IET Conference Publications*, vol. 2018, no. CP740, 2018, doi: 10.1049/cp.2018.0002.

[40] E. Kwarteng and M. Cebe, "A survey on security issues in modern Implantable Devices: Solutions and future issues," *Smart Health*, vol. 25, no. June, p. 100295, 2022

[41] F. Janjua, A. Masood, H. Abbas, and I. Rashid, "Handling insider threat through supervised machine learning techniques," *Procedia Comput Sci*, vol. 177, pp. 64–71, 2020, doi: 10.1016/j.procs.2020.10.012.

[42] L. Cheng, F. Liu, and D. D. Yao, "Enterprise data breach: causes, challenges, prevention, and future directions," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 7, no. 5. Wiley-Blackwell, Sep. 01, 2017. doi: 10.1002/widm.1211.

[43] B. Abd-El-Atty, "A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks," *Neural Comput Appl*, vol. 35, no. 1, pp. 773–785, 2023, doi: 10.1007/s00521-022-07830-0.

[44] Q. Chen, J. Lambright, and S. Abdelwahed, "Towards Autonomic Security Management of Healthcare Information Systems," *Proceedings - 2016 IEEE 1st International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE 2016*, pp. 113–118, 2016, doi: 10.1109/CHASE.2016.58.

[45] G. Bell and M. Ebert, "Health care and Cyber Security: Increasing Threats Require Increased Capabilities," 2018.

[46] Skillnet, "Cybersecurity Skills Development Strategy," 2021. [Online].Available:https://www.skillnetireland.ie/publication/cybersecurity-skills-development-strategy-itcork-skillnet/

[47] D. Mohammed, R. Mariani, and S. Mohammed, "Cybersecurity Challenges and Compliance Issues within the U.S. Healthcare Sector," *International Journal of Business and Social Research*, vol. 5, no. 2, pp. 55–66, 2015.

[48] W. L. Holden, "Bridging the culture gap between healthcare it and medical device development," *Biomed Instrum Technol*, vol. 48, no. Horizons, pp. 22–28, 2014, doi: 10.2345/0899-8205-48.s2.22.

[49] J. Q. Chen and A. Benusa, "HIPAA security compliance challenges: The case for small healthcare providers," *Int J Healthc Manag*, vol. 10, no. 2, pp. 135–146, 2017

[50] K. Townsend, "Organizations Challenged with Cybersecurity Framework Implementation," *Security Week*, 2017. https://www.securityweek.com/organizations-challenged-cybersecurity-framework-implementation/ (accessed Aug. 15, 2023).

[51] AAMI TIR 57, "Principles for medical device security—Risk management," 2016.

[52] FDA, "Cybersecurity in Medical Devices : Quality System Considerations and Content of Premarket Submissions," 2022.

[53] FDA, "Postmarket Management of Cybersecurity in Medical Devices," pp. 1–30, 2016.

[54] P. C. Paul, J. Loane, F. McCaffery, and G. Regan, "Towards design and development of a data security and privacy risk management framework for wban based healthcare applications," *Applied System Innovation*, vol. 4, no. 4, pp. 704–710, 2021

[55] H. Zhao and G. Yang, "Information Security and Legal Ethics of Artificial Intelligence Medical Devices.pdf," *Forest Chemicals Review*, 2022.

[56] T. Granlund, J. Vedenpaa, V. Stirbu, and T. Mikkonen, "On Medical Device Cybersecurity Compliance in EU," *Proceedings - 2021 IEEE/ACM 3rd International Workshop on Software Engineering for Healthcare, SEH 2021*, pp. 20–23, 2021

[57] S. Togneri, T. Cooper, and F. McCaffery, "Revising IEC 80001-1 : Risk management of health information technology systems," *Comput Stand Interfaces*, vol. 60, no. May, pp. 67–72, 2018.

[58] M. Musser, J. Spring, A. Lohn, C. Martinez, J. X. Dempsey, and C. D. Grant, "Adversarial Machine Learning and Cybersecurity: Risks, Challenges, and Legal Implications," 2023.

[59] BS/AAMI 34971, "Application of BS EN ISO 14971 to machine learning in artificial intelligence – Guide," 2023.