International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 06 | Jun 2026 www.irjet.net p-ISSN: 2395-0072

AI in the Medical Sector and Data Privacy in Healthcare

Talal Mubarak Al-Harbi

College of Computing, Fahad Bin Sultan University, AIMD Lab, KSA, Tabuk

---

Abstract - *This research analyses artificial intelligence in the medical sector and healthcare data privacy as two interdependent areas of modern digital health. AI is increasingly applied in medical imaging, clinical decision support, hospital operations, patient monitoring and documentation. These applications can improve efficiency, consistency and access to care, but they also raise concerns about bias, safety, explain ability, regulation and professional responsibility. At the same time, medical AI depends on large volumes of sensitive patient data, including electronic health records, images, laboratory results and clinical notes. Healthcare data privacy is therefore essential for lawful, ethical and trustworthy AI development. The research explains medical AI concepts, major applications, benefits and limitations, then discusses privacy principles, protected health information, de-identification, data governance and patient rights. It concludes that medical AI should be deployed only when clinical value, patient safety, privacy protection and accountability are addressed throughout the full lifecycle from data collection to post-market monitoring.*

Key Words: AI in the Medical Sector, Data Privacy in Healthcare, governance, risk management, digital systems.

1. INTRODUCTION

Artificial intelligence is increasingly used in healthcare for medical imaging, clinical decision support, triage, administrative automation, drug discovery and patient monitoring. These applications can improve speed, consistency and access to care, but they also create risks because medical decisions are high-stakes and health data is sensitive [1]. A technical error in a recommendation system can affect patient safety, while weak privacy governance can expose protected health information.

This research studies AI in the Medical Sector and Data Privacy in Healthcare. The two topics are connected because most medical AI systems depend on patient data for training, validation and deployment. Health records, imaging scans, laboratory results, clinician notes and wearable-device data can be valuable for model development, but they must be processed under strict legal ethical and security requirements. The research therefore considers both the promise of medical AI and the safeguards needed to protect patient rights.

The research focuses on practical academic analysis rather than technical implementation. It explains core AI applications in healthcare, benefits and limitations, regulatory and clinical concerns, healthcare data privacy principles, and recommendations for responsible adoption. The main argument is that medical AI should be developed as a socio-technical system: the model, the data, the clinicians, the patients, the workflow and the governance structure all influence safety and trust.

2. AI IN THE MEDICAL SECTOR - BACKGROUND AND CONCEPTS

AI in medicine refers to computational systems that perform tasks normally requiring human intelligence, such as pattern recognition, prediction, classification and decision support. In healthcare, AI may analyse radiology images, identify high-risk patients, assist clinical documentation, detect abnormal physiological signals or support personalized treatment planning. Machine learning and deep learning are especially important because many medical datasets are complex and high-dimensional [2. 3. 4]. In terms of expected growth of AI in medical sector, Figure 1 provides important information.

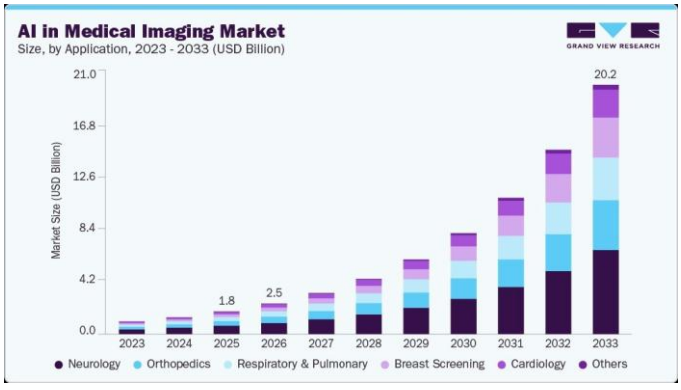

Figure-1: The Rapid Growth of AI in Medical Imaging

Figure 1 shows the expected growth of the AI in medical imaging market from 2023 to 2033, measured in USD billions. It presents different application areas, including neurology, orthopedics, respiratory and pulmonary, breast screening, cardiology, and others. The chart indicates a continuous and rapid increase in market size over the years. The market is shown growing from a relatively small value in 2023 to about 20.2 billion USD by 2033. This growth reflects the increasing adoption of AI technologies in medical imaging for diagnosis, screening, disease detection, and clinical decision support. Therefore, the

figure highlights that AI is becoming an important part of healthcare, especially in imaging-based medical applications, where it can improve accuracy, speed, and efficiency in clinical services.

The WHO emphasizes that AI for health should promote safety, equity, transparency and accountability [5]. This is important because medical AI is not merely a software tool; it interacts with clinical judgement, professional responsibility and patient outcomes. The NIST AI Risk Management Framework similarly encourages organizations to manage AI risks through governance, mapping, measurement and management of system impacts [6]. These frameworks show that trustworthy AI requires more than accuracy metrics. (World Health Organization, 2024)

Medical AI development usually follows a lifecycle. It begins with a clinical problem, continues with data curation and model training, proceeds to validation and regulatory review, and then enters real clinical use with monitoring. Each stage has risks. Poorly curated data can produce biased models. Validation on a narrow population may fail when the model is used in a different hospital. Lack of post-deployment monitoring can allow model drift to remain unnoticed.

AI can be descriptive, predictive, diagnostic or generative. Descriptive systems summarize data; predictive systems estimate risk; diagnostic systems classify or detect disease; generative systems can produce text, images or recommendations. Large multi-modal models are a newer category because they can process multiple types of input, such as text, images and signals. Their flexibility creates new opportunities but also raises concerns about hallucination, explain ability and clinical accountability.

3. AI APPLICATIONS, BENEFITS, AND CHALLENGES

Before presenting applications of AI in medical sector, it is worth mentioning that the applications are tightly-coupled with: 1) security of web applications as all advanced medical centers use online services [7]; and 2) with big data that requires effective analyzing [8]. One major application is medical imaging. AI systems can assist in detecting abnormalities in X-rays, CT, MRI, ultrasound and pathology slides. These tools may reduce workload and support early detection, especially in settings with limited specialist availability. However, imaging AI must be validated across scanner types, patient populations and clinical workflows. A model that performs well in one dataset may not generalize to another hospital if acquisition protocols or patient demographics differ.

Clinical decision support is another important application [9]. Predictive models can estimate deterioration risk, sepsis risk, readmission probability or medication interaction concerns. Such systems can help clinicians prioritize attention, but they should not replace professional judgement. Alert fatigue, false positives, false negatives and unclear explanations can reduce the usefulness of decision support. Human oversight remains essential.

AI also supports administrative and operational functions, such as appointment scheduling, billing assistance, documentation, bed management and resource allocation [10]. These uses may reduce costs and improve efficiency. Compared with diagnostic AI, administrative AI may appear lower-risk, but it can still produce unfair outcomes if scheduling, triage or eligibility decisions are biased.

The major challenges include data quality, bias, explain ability, clinical validation, regulatory approval, liability and integration into workflows. Healthcare data is often incomplete, inconsistent or biased toward populations that have better access to care. AI may reproduce these patterns. Therefore, medical AI must be evaluated not only for average accuracy but also for subgroup performance, fairness, usability and safety.

4. DATA PRIVACY IN HEALTHCARE - BACKGROUND AND CONCEPTS

Healthcare data privacy concerns the protection of information that can identify a patient or reveal health status, treatment, diagnosis, medication, genetic data or care history. Health information is sensitive because disclosure can cause discrimination, stigma, financial harm and loss of trust. This can be highlighted when using location based services to search for nearest hospitals or medical centers [11, 12]. Privacy protection is therefore a foundation of ethical healthcare and a condition for patient willingness to share accurate information [13].

The HIPAA Privacy Rule establishes national standards in the United States for protecting medical records and other individually identifiable health information [14]. Although legal details vary by jurisdiction, the broader principles are widely relevant: access should be limited, uses and disclosures should be justified, patients should have rights over their information and healthcare organizations must safeguard records. The GDPR similarly treats health data as a special category of personal data requiring strong protections. (European Commission, n.d.) Healthcare privacy is not only about legal compliance. It is also about data governance across the entire AI pipeline. Data may move from electronic health records to research databases, annotation platforms, model training environments, cloud services and clinical dashboards. Each transfer can introduce risk. Privacy governance must therefore include

data mapping, access control, de-identification, audit logging, secure storage and clear accountability.

De-identification is useful but not a complete solution. Medical datasets can contain rare diagnoses, images, timestamps and combinations of attributes that may enable re-identification. For AI research, organizations should assess re-identification risk, limit data access, use data-use agreements and consider privacy-preserving methods such as federated learning, secure enclaves or synthetic data where appropriate.

5. PRIVACY APPLICATIONS, BENEFITS, AND CHALLENGES

Privacy safeguards support responsible medical AI by allowing data to be used for public benefit while reducing harm to individuals. For example, a hospital may create a governed dataset for training an imaging model, but it should remove direct identifiers, document consent or legal basis, restrict researcher access and maintain audit logs. A healthcare network may also use federated learning so that models learn from multiple institutions without centralizing raw patient data.

The benefits of strong healthcare data privacy include patient trust, legal compliance, reduced breach risk and higher-quality research governance. Patients are more likely to participate in digital health systems when they believe their information is protected. Clinicians are also more likely to trust AI tools when data provenance and governance are clear.

The challenges include the complexity of health data, interoperability demands, secondary data use, cloud outsourcing and consumer health technologies. Wearables, mobile health apps and wellness platforms may collect health-related data outside traditional hospital privacy frameworks. This creates gaps between medical privacy expectations and actual data practices. AI intensifies this issue because data collected for one purpose may be attractive for model development.

Another challenge is the tension between privacy and data utility. Strong anonymization may reduce clinical detail, while detailed data may increase privacy risk. The solution is not to abandon data use, but to apply proportionate safeguards based on risk. High-risk datasets require stronger controls, independent review and continuous monitoring. Figure 2 reflects the previous information in terms of bar char.

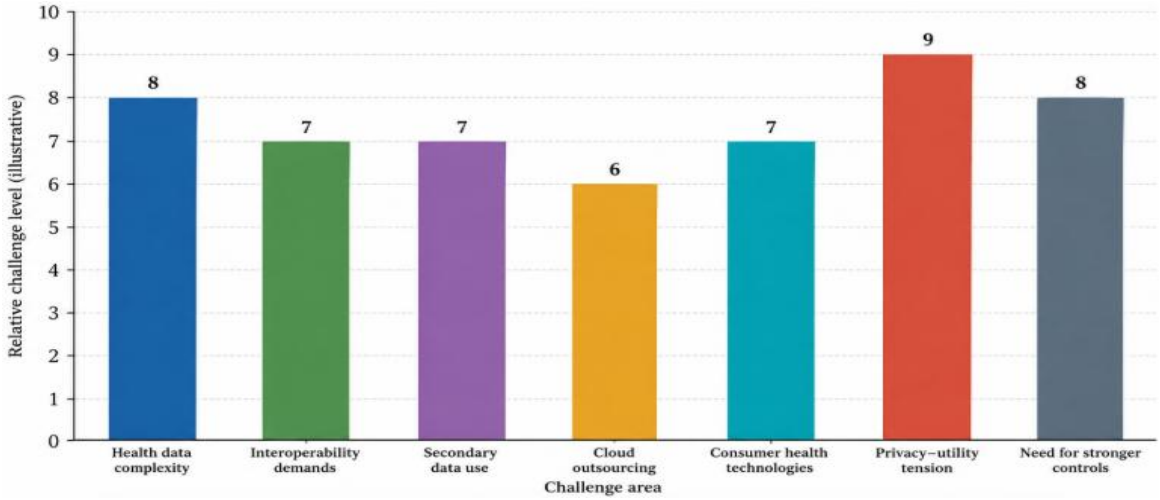

Figure-2: Key challenges in healthcare data privacy and AI use.

Sub-challenges can be explored when using agent-based systems to serve medical systems. They are related to search for moving points of interests like emergency medical cars based on location based services [15], attacks that may negatively affect IoT-based systems [16], load balancing of energy of mobile devices when executing privacy protection systems [17], and security of agents when migrating from home machine (mobile device, PC, or smart watch of patients) to the destination machines like medical health providers [18, 19, 20].

6. COMPARATIVE DISCUSSION

AI in the medical sector and healthcare data privacy are inseparable. Medical AI needs data to learn patterns, but healthcare privacy defines the boundaries of acceptable data use. A model trained on poorly governed patient data may achieve technical performance but still be ethically unacceptable. Conversely, privacy rules that are implemented without understanding AI requirements may unnecessarily block beneficial research. The task is to combine innovation with responsible governance.

The two topics also share a lifecycle perspective. AI requires monitoring from development to deployment; privacy requires protection from collection to deletion. In both cases, one-time approval is insufficient. Models can drift, data practices can change, vendors can be replaced and regulations can evolve. Healthcare organizations therefore need continuous governance rather than isolated compliance documents.

A balanced medical AI programme should ask three questions: Is the AI clinically useful and safe? Is the patient data processed lawfully and fairly? Is there accountability if the system fails or causes harm? These questions show that the ethical value of medical AI depends on both technical performance and trustworthy data stewardship.

7. ETHICAL, LEGAL, AND PROFESSIONAL CONSIDERATIONS

The ethical issues in medical AI include patient safety, informed use, bias, explain ability, human oversight and accountability. AI systems should not be deployed simply because they are technologically impressive. They should solve clinically meaningful problems and demonstrate evidence of benefit. Patients and clinicians should know when AI is involved in care, especially when recommendations influence diagnosis or treatment.

Legal and regulatory considerations include health privacy laws, medical device regulation, data protection requirements and institutional review. The FDA has issued guidance and resources for AI-enabled medical device software, including lifecycle management and transparency principles. Such guidance reflects the fact that AI-enabled medical devices may change over time and require careful post-market controls. (Food and Drug Administration, 2025)

Professional responsibility belongs to developers, hospitals, clinicians, administrators and regulators. Developers must document data sources, limitations and validation. Hospitals must evaluate whether a system fits their patients and workflow. Clinicians must understand when to rely on or challenge AI output. Regulators and ethics committees must ensure that safety and privacy are not sacrificed for speed of innovation.

8. RECOMMENDATIONS

Healthcare organizations should begin with clinically justified AI use cases rather than technology-driven experimentation. Each project should define the clinical problem, expected users, intended patient population, data requirements and risk level. Before deployment, AI tools should be externally validated where possible and assessed for subgroup performance, bias, usability and safety.

Data privacy governance should include data inventories, access controls, de-identification, audit logs, retention schedules and data-use agreements. For high-risk AI development, institutions should consider privacy-preserving approaches such as federated learning, secure research environments or limited-data access models. Cloud vendors should be evaluated through security and privacy requirements, not only cost and functionality.

Clinicians should receive training on AI strengths and limitations. Patients should receive transparent information when AI meaningfully contributes to care. Finally, medical AI should be monitored after deployment for performance drift, adverse events, workflow problems and privacy incidents. Responsible adoption is a continuous process, not a one-time purchase.

9. CONCLUSION

AI offers significant opportunities for healthcare, including improved diagnostic support, operational efficiency, risk prediction and access to expertise. However, these benefits depend on safe development, clinical validation, human oversight and trustworthy data governance. Healthcare data is among the most sensitive categories of personal information, and AI increases both the value and the risk of such data.

The key conclusion is that medical AI and healthcare data privacy must be managed together. A useful AI system must also be lawful, fair, secure and accountable. The future of AI in medicine should be guided by patient benefit, clinical evidence, privacy protection and public trust.

ACKNOWLEDGEMENT

The author used ChatGPT to assist in preparing illustrative figures and proofreading the manuscript. However, the core scientific content was developed and presented by the author.

REFERENCES

[1] Obuchowicz, Rafał, Michał Strzelecki, and Adam Piórkowski. "Clinical applications of artificial intelligence in medical imaging and image processing—A review." Cancers 16.10 (2024): 1870.

[2] Mona Alfifi, Mohamad Shady Alrahhal, Samir Bataineh and Mohammad Mezher, "Enhanced Artificial Intelligence System for Diagnosing and Predicting Breast Cancer using Deep Learning," International Journal of Advanced Computer Science and Applications, vol. 11, no. 7, 2020.

[3] Mohamad Shady Alrahhal and Eftkhar Alqhtani, "Deep learning-based system for detection of lung cancer using fusion of features," International Journal of

Computer Science and Mobile Computing, vol. 10, no. 2, pp. 57-67, 2021.

[4] Mohamad Shady Alrahhal and Majed Abdullah Albarrk, "A Survey of the COVID-19 Epidemic Through the Eyes of Artificial Intelligence and Deep Learning: Challenges and Research Questions," 2020.

[5] World Health Organization. Ethics and governance of artificial intelligence for health: WHO guidance. World Health Organization, 2021.

[6] Dotan, Ravit, et al. "Evolving AI risk management: A maturity model based on the NIST AI risk management framework." arXiv preprint arXiv:2401.15229 (2024).

[7] Majed Abdullah Albarrk and Mohamad Shady Alrahhal, "Web Applications Security: More Collaboration," 2020.

[8] Mohamad Shady Alrahhal and Adnan Abi Sen, "Data mining, big data, and artificial intelligence: An overview, challenges, and research questions," 2018.

[9] Sutton, Reed T., et al. "An overview of clinical decision support systems: benefits, risks, and strategies for success." NPJ digital medicine 3.1 (2020): 17.

[10] Saravanan, K., et al. "AI for Hospital Administration, Staff Scheduling, and Operational Efficiency: Transforming Healthcare Operations Through Intelligent Automation." Breakthroughs in Smart Nursing With Generative AI. IGI Global Scientific Publishing, 2026. 213-240.

[11] Mohamad Shady Alrahhal, Muhammad Usman Ashraf, Adnan Abesen and Sabah Arif, "AES-Route Server Model for Location Based Services in Road Networks," International Journal of Advanced Computer Science and Applications, vol. 8, no. 8, 2017.

[12] Hosam Alrahhal et al., "A symbiotic relationship based leader approach for privacy protection in location based services," ISPRS International Journal of Geo-Information, vol. 9, no. 6, p. 408, 2020.

[13] Mohamad Shady Alrahhal, Maher Khemakhem and Kamal Jambi, "A Survey on Privacy of Location-Based Services: Classification, Inference Attacks, and Challenges," Journal of Theoretical and Applied Information Technology, vol. 95, no. 24, 2017.

[14] Moore, Wilnellys, and Sarah Frye. "Review of HIPAA, part 1: history, protected health information, and privacy and security rules." Journal of nuclear medicine technology 47.4 (2019): 269-272.

[15] Mohamad Shady Alrahhal, Maher Khemakhem and Kamal Jambi, "Agent-Based System for Efficient kNN Query Processing with Comprehensive Privacy Protection," International Journal of Advanced Computer Science and Applications, vol. 9, no. 1, 2018.

[16] Abdullah S. Alyousef, Karthik Srinivasan, Mohamad Shady Alrahhal, Majdah Alshammari and Mousa Al-Akhras, "Preserving Location Privacy in the IoT against Advanced Attacks using Deep Learning," International Journal of Advanced Computer Science and Applications, vol. 13, no. 1, 2022.

[17] Mohamad Shady Alrahhal, Maher Khemekhem and Kamal Jambi, "Achieving load balancing between privacy protection level and power consumption in location based services," International Research Journal of Engineering and Technology, vol. 5, no. 3, pp. 619-625, 2018.

[18] Bandar Alluhaybi, Mohamad Shady Alrahhal, Ahmed Alzhrani and Vijey Thayananthan, "A Survey: Agent-based Software Technology Under the Eyes of Cyber Security, Security Controls, Attacks and Challenges," International Journal of Advanced Computer Science and Applications, vol. 10, no. 8, 2019.

[19] Bandar Alluhaybi, Mohamad Shady Alrahhal, Ahmed Alzhrani and Vijey Thayananthan, "Dummy-based approach for protecting mobile agents against malicious destination machines," IEEE Access, vol. 8, pp. 129320-129337, 2020.

[20] Bandar Alluhaybi, Mohamad Shady Alrahhal, Ahmed Alzhrani and Vijey Thayananthan, "Achieving self-protection and self-communication features for security of agent-based systems," 2020.