ISSN 2616-5902 Vol. 8, Issue 4: 105-110, DOI: 10.25236/AJBM.2026.080414

Privacy Security Risks and Governance Mechanisms of Medical Imaging Data in the Context of Artificial Intelligence

Fugen Zhou[1,a], Shangying Zhou[2,b]

[1]*School of Health Science and Engineering, University of Shanghai for Science and Technology, Shanghai, China*
[2]*School of Business, University of Shanghai for Science and Technology, Shanghai, China*
[a]*Zhoufg1999@qq.com,* [b]*1095963826@qq.com*

Abstract: *With the rapid development of artificial intelligence (AI) technologies in the healthcare sector, medical imaging data have been increasingly applied in disease diagnosis, clinical decision-making, and medical research, becoming a critical foundational resource for the advancement of smart healthcare. However, due to their high sensitivity and identifiability, the large-scale circulation of medical imaging data across processes such as collection, storage, processing, and sharing has significantly intensified privacy security risks. From the perspective of the data lifecycle, this study systematically analyzes the privacy risks associated with medical imaging data at different stages under the AI context and explores their underlying causes from technological, institutional, and behavioral dimensions. On this basis, a comprehensive governance framework is constructed, encompassing technological governance, institutional governance, organizational governance, and multi-stakeholder collaborative governance. The findings indicate that privacy risks of medical imaging data exhibit full lifecycle penetration and multi-factor coupling characteristics. Therefore, achieving a balance between data utilization and privacy protection requires a multi-level coordinated governance approach. This study provides theoretical insights for improving healthcare data governance systems and promoting the sustainable development of intelligent healthcare.*

Keywords: *Artificial Intelligence, Medical Imaging Data, Privacy Security, Data Governance*

1. Introduction

Against the backdrop of the rapid development of the digital economy and artificial intelligence technologies, the healthcare sector is undergoing profound transformation. AI technologies, particularly deep learning and computer vision, have been widely applied in medical imaging analysis, disease diagnosis, and clinical decision support, significantly enhancing both efficiency and accuracy in healthcare services. As a key resource for AI-driven healthcare applications, medical imaging data—including CT, MRI, and X-ray images—are characterized by high information density, complex structures, and significant clinical value, gradually becoming a core production factor in the development of smart healthcare.

At the same time, the large-scale circulation of medical imaging data throughout their lifecycle—ranging from collection and storage to processing and sharing—has led to increasingly severe privacy security challenges. Compared with general data, medical imaging data not only contain detailed health information but may also enable individual identification through techniques such as facial reconstruction, thereby exhibiting high sensitivity and identifiability. Once data leakage or misuse occurs, it may not only infringe upon patients' privacy rights but also undermine trust in healthcare systems and trigger broader ethical concerns.

Existing studies have primarily examined privacy protection from single perspectives such as data security technologies or legal regulation. However, under the deep integration of AI into medical imaging applications, traditional governance approaches face significant limitations.[1] On the one hand, conventional de-identification methods are insufficient for high-dimensional imaging data and remain vulnerable to re-identification.[2] On the other hand, AI models themselves may become new carriers of privacy leakage, with emerging risks such as model inversion attacks. [3] Furthermore, existing legal and regulatory frameworks lag behind technological developments, particularly in areas such as data

ISSN 2616-5902 Vol. 8, Issue 4: 105-110, DOI: 10.25236/AJBM.2026.080414

ownership and cross-institutional data governance.

Therefore, this study focuses on privacy security issues in medical imaging data within the AI context. Based on the data lifecycle perspective, it systematically identifies privacy risks and analyzes their underlying causes across different application scenarios. Furthermore, a multi-level collaborative governance framework integrating technological, institutional, and organizational mechanisms is proposed to achieve a balance between data usability and controllability, thereby providing theoretical and practical support for the development of intelligent healthcare.

2. Applications of Medical Imaging Data in the AI Context

Driven by AI technologies, the application scope of medical imaging data has expanded significantly, evolving from traditional diagnostic tools into essential resources that support the entire healthcare service process. From the perspectives of functional application and data flow, medical imaging data are primarily utilized in intelligent diagnosis, medical research, data-sharing platforms, and commercial applications.

2.1. Intelligent Assisted Diagnosis

In clinical practice, intelligent assisted diagnosis represents the most fundamental application of medical imaging data. AI models based on deep learning can automatically analyze CT, MRI, and X-ray images, enabling rapid detection and classification of diseases such as tumors, lung nodules, and cardiovascular conditions.

Compared with traditional diagnosis relying on physicians' experience, AI-driven approaches significantly improve diagnostic efficiency and accuracy, particularly in resource-constrained settings. However, this application scenario requires large-scale, high-quality datasets, thereby increasing the risk of privacy exposure during data collection and usage.[4]

2.2. Medical Research and AI Model Training

Medical imaging data play a foundational role in medical research and AI model training. By analyzing large-scale datasets, researchers can uncover disease patterns and support the development of precision medicine. Meanwhile, high-quality labeled data are essential for improving model performance.

In this context, data are often integrated across time and populations and reused multiple times. While such practices enhance data value, they also prolong the exposure period and increase the risk of privacy leakage and re-identification.[5]

2.3. Data Sharing and Platform-Based Applications

With the advancement of healthcare informatization, medical imaging data are increasingly shared across institutions through digital platforms, such as regional healthcare information systems and cloud-based services. This facilitates efficient allocation of medical resources.

However, extended data transmission chains involving multiple entities significantly increase security risks. Moreover, differences in data standards and security capabilities among institutions further exacerbate uncertainties in data protection.[6]

2.4. Commercial and Industrial Applications

In the context of AI industrialization, medical imaging data are increasingly regarded as valuable data assets. Technology companies collaborate with healthcare institutions to develop AI-based diagnostic systems and health management platforms.

Additionally, such data may be used in insurance, risk assessment, and personalized services. While expanding application boundaries, these practices also raise concerns about data misuse and excessive commercialization, particularly when data are used without proper authorization.[7]

Furthermore, Chinese scholarship highlights the role of digital transformation, supply chain digital infrastructure, big-data platforms, and intelligent manufacturing in building resilience. China's system-wide digital infrastructure, industrial-chain integration capabilities, and platform economy have

ISSN 2616-5902 Vol. 8, Issue 4: 105-110, DOI: 10.25236/AJBM.2026.080414

contributed to unique pathways of resilience development, offering localized insights that enrich global resilience theory.

3. Privacy Security Risk Analysis of Medical Imaging Data

3.1. Privacy Risks in the Data Collection Stage

At the data collection stage, medical imaging data are primarily generated through diagnostic imaging procedures conducted by healthcare institutions. The major privacy risks at this stage stem from insufficient informed consent and excessive data collection.[8]

First, some healthcare institutions fail to fully fulfill their obligation of informed consent during data collection. Patients often lack a clear understanding that their imaging data may subsequently be used for research or commercial purposes, resulting in data usage that exceeds the scope of the original authorization.

Second, driven by the demand for high-performance AI models, institutions tend to collect large volumes of high-dimensional imaging data. This practice of "over-collection" expands the potential exposure surface of sensitive information. If such data are not properly managed, it may lead to large-scale privacy breaches.

3.2. Privacy Risks in the Data Storage Stage

Medical imaging data are typically stored in large volumes within hospital information systems or cloud platforms. This centralized storage model makes them prime targets for cyberattacks.[9]

On the one hand, inadequate security protection mechanisms in database systems may expose them to threats such as hacking and ransomware attacks, resulting in unauthorized access or data tampering. On the other hand, internal misuse of access privileges constitutes another critical risk source, as staff may access or copy sensitive imaging data without proper authorization.

Furthermore, in cloud storage environments, cross-domain data storage may introduce additional vulnerabilities due to variations in the security capabilities of service providers, thereby increasing the likelihood of data leakage.

3.3. Privacy Risks in the Data Processing Stage

During the data processing stage, medical imaging data are typically subjected to annotation, cleaning, and de-identification in order to meet the requirements of AI model training. However, this stage presents significant privacy risks.

First, traditional de-identification methods, such as removing explicit identifiers (e.g., names or identification numbers), are insufficient to fully eliminate privacy risks. Due to the inherent uniqueness of medical imaging data, certain images—such as cranial CT or MRI scans—can be used to reconstruct facial features through three-dimensional modeling, thereby enabling re-identification.

Second, AI models may "memorize" features of the original training data during the learning process. Attackers can exploit techniques such as model inversion and membership inference to extract sensitive information from trained models, thereby creating new pathways for privacy leakage.

3.4. Privacy Risks in the Data Sharing and Transmission Stage

With the increasing integration of healthcare data resources and the expansion of cross-institutional collaboration, medical imaging data are being shared and transmitted more frequently across different entities, making this stage particularly vulnerable.

On the one hand, as data flow across hospitals, regions, and even national borders, the length and complexity of transmission chains increase, raising the risk of interception or tampering. On the other hand, third-party technology platforms, such as AI companies and cloud service providers, may misuse data beyond authorized scopes due to insufficient regulation or profit-driven incentives.

Moreover, the lack of unified data standards and security protocols among institutions further exacerbates uncertainties and risks in the data-sharing process.

ISSN 2616-5902 Vol. 8, Issue 4: 105-110, DOI: 10.25236/AJBM.2026.080414

3.5. Privacy Risks in the Data Application Stage

At the data application stage, medical imaging data are widely used in AI model training, clinical decision support, and commercial development. The associated privacy risks at this stage are characterized by their concealment and long-term impact.

First, some enterprises may use medical imaging data for commercial purposes—such as insurance pricing or targeted marketing—without proper patient authorization, leading to data misuse.

Second, AI models trained on medical imaging data may exhibit biases across different population groups, potentially resulting in algorithmic discrimination and ethical concerns.

Finally, once data are incorporated into irreversible model training processes, their influence cannot be fully eliminated even if the original data are subsequently deleted, thereby increasing the persistence and long-term nature of privacy risks.

4. Governance Mechanisms for Privacy Security of Medical Imaging Data in the Context of Artificial Intelligence

Given the multi-dimensional privacy security risks exhibited throughout the lifecycle of medical imaging data, relying solely on a single governance approach is insufficient for effective risk mitigation. In the context of the continuous advancement of artificial intelligence technologies, it is necessary to establish a comprehensive governance framework that integrates technological governance as the foundation, institutional governance as the guarantee, organizational governance as the support, and multi-stakeholder collaboration as a complementary mechanism. Such an approach aims to achieve a dynamic balance between data security and value utilization.

4.1. Technological Governance: A Privacy-Computing-Oriented Security Pathway

Technological measures constitute the first line of defense against privacy risks in medical imaging data. In AI applications, various privacy-preserving technologies should be employed to ensure that data remain “usable but not visible.”

First, in the data processing stage, data desensitization and anonymization techniques should be strengthened. Both explicit and implicit identity-related information in medical imaging data should be addressed through multi-layered processing methods, such as removing metadata identifiers and blurring facial features, in order to reduce the risk of re-identification.

Second, differential privacy can be introduced to protect individual data characteristics by adding controlled random noise during data analysis or model training, thereby preserving overall data utility while preventing privacy leakage.

In addition, federated learning has emerged as an important technological approach in recent years. It enables collaborative model training across institutions without sharing raw data, thereby effectively mitigating the risks associated with centralized data storage.

Furthermore, blockchain technology can be explored in medical data management. By leveraging distributed ledger systems, blockchain can ensure the traceability and immutability of data access records, thereby enhancing transparency and trust in data usage processes.

Overall, the core of technological governance lies in leveraging privacy computing and secure architecture design to establish a new data utilization paradigm characterized by “data remaining in local domains while models are shared across entities.”

4.2. Institutional Governance: Improving Legal Frameworks and Regulatory Systems

Institutional governance provides a fundamental guarantee for the protection of medical imaging data privacy. In the AI context, it is essential to strengthen the regulation and governance of medical data through comprehensive legal and policy frameworks.

First, existing laws and regulations related to medical data privacy protection should be further improved. This includes clarifying the legal attributes and ownership boundaries of medical imaging data, specifying the permissible scope of data collection, use, and sharing, and strengthening legal accountability for unauthorized data usage.

ISSN 2616-5902 Vol. 8, Issue 4: 105-110, DOI: 10.25236/AJBM.2026.080414

Second, unified data security standards and technical specifications should be established. Standardization across healthcare institutions in terms of data formats, de-identification processes, and security protocols can significantly reduce risks during data circulation.

Moreover, regulatory authorities should enhance full-lifecycle supervision of medical data flows, particularly in cross-institutional and cross-regional data-sharing scenarios, by establishing dynamic monitoring and risk assessment mechanisms. At the same time, third-party auditing mechanisms can be introduced to independently evaluate data usage practices of healthcare institutions and technology companies, thereby improving the effectiveness of institutional enforcement.

4.3. Organizational Governance: Strengthening Internal Management Capacity of Healthcare Institutions

As the primary holders and users of medical imaging data, healthcare institutions play a critical role in privacy governance. Therefore, it is necessary to improve internal governance systems at the organizational level to enhance data security management capabilities.

First, a comprehensive data classification and grading management system should be established. Based on the sensitivity and usage scenarios of medical imaging data, differentiated management strategies should be implemented, clearly defining access permissions and usage scopes for different data levels.

Second, data access control mechanisms should be strengthened. Through identity authentication, permission allocation, and logging systems, the entire process of data access can be effectively monitored, thereby preventing internal misuse.

In addition, healthcare institutions should enhance data security awareness through regular training programs, improving the privacy protection awareness and compliance capabilities of both medical and technical personnel. Furthermore, an emergency response mechanism for data security incidents should be established, enabling timely risk mitigation and accountability tracing in the event of data breaches.

4.4. Multi-Stakeholder Collaborative Governance: Building a Co-Governance Data Ecosystem

The application of medical imaging data involves multiple stakeholders, including government regulators, healthcare institutions, technology enterprises, and patients. Therefore, effective governance cannot rely on a single entity, but requires a collaborative, multi-stakeholder approach.

Government agencies should play a leading role by establishing policies, regulations, and regulatory standards to provide an institutional framework for data governance. Healthcare institutions, as primary data sources, should strengthen data management and security protection. Technology enterprises should assume the responsibility of technological empowerment by providing secure and reliable data processing and analysis tools. Meanwhile, patients, as data subjects, should be granted rights to informed consent and data usage choices, and should participate in governance oversight.

In addition, the development of data-sharing platforms or data exchange mechanisms can be explored to facilitate the rational circulation of data resources under the premise of privacy protection. Through collaborative efforts among multiple stakeholders, a data governance ecosystem characterized by clear responsibilities and efficient operation can be gradually established.

5. Conclusion and Future Research

5.1. Research Conclusions

In the context of the rapid advancement of artificial intelligence technologies, medical imaging data have emerged as a critical foundational resource for intelligent healthcare, with continuously expanding application value. However, this development has also introduced increasingly complex privacy security challenges. Focusing on privacy security issues in AI-driven applications of medical imaging data, this study systematically identifies and analyzes privacy risks from the perspective of application scenarios and the data lifecycle.

The findings indicate that privacy risks associated with medical imaging data permeate the entire lifecycle, including data collection, storage, processing, sharing, and utilization, and exhibit characteristics of multi-stage accumulation and cross-entity transmission. Among these risks, insufficient

ISSN 2616-5902 Vol. 8, Issue 4: 105-110, DOI: 10.25236/AJBM.2026.080414

de-identification, model inversion threats, uncontrolled cross-institutional data flows, and data misuse are particularly prominent. Furthermore, the emergence of privacy risks cannot be attributed to a single factor; rather, it results from the combined effects of technological limitations, institutional lag, imbalanced stakeholder behavior, and the inherent high sensitivity and mobility of medical imaging data.

Based on these findings, this study constructs a multi-level governance framework for the privacy security of medical imaging data in the AI context. It proposes that technological measures, particularly privacy-preserving techniques such as differential privacy and federated learning, should serve as the foundation for secure data utilization. Institutional frameworks, including legal regulations and standardized systems, should provide essential safeguards by clarifying data ownership and usage boundaries. Organizational governance within healthcare institutions should be strengthened through data classification and access control mechanisms. Moreover, collaborative participation among multiple stakeholders—including governments, healthcare institutions, technology enterprises, and patients—is necessary to establish a systematic and coordinated data governance system. This governance framework contributes to safeguarding privacy while fully unlocking the application value of medical imaging data.

5.2. Limitations and Future Research

This study provides a systematic, multi-dimensional analysis of privacy and security issues in medical imaging data, yet several limitations remain. The research is primarily theoretical, lacking empirical validation; future studies should incorporate real-world data to test the proposed governance framework. Meanwhile, rapid advancements in artificial intelligence continue to introduce emerging privacy risks—such as data leakage from generative models and privacy reconstruction via cross-modal integration—that require further investigation. In addition, the growing prevalence of cross-border medical data flows highlights challenges arising from differences in international regulatory frameworks, underscoring the need for more coordinated and globally harmonized data governance approaches.

References

[1] Murdoch, B. (2021). Privacy and artificial intelligence: challenges for protecting health information in a new era. BMC Medical Ethics, 22.
[2] Rempe, M., Heine, L., Seibold, C., Hörst, F., & Kleesiek, J. (2024). De-identification of medical imaging data: a comprehensive tool for ensuring patient privacy. European Radiology, 35, 7809 - 7818.
[3] Kaissis, G., Ziller, A., Passerat-Palmbach, J., Ryffel, T., Usynin, D., Trask, A., Lima, I., Mancuso, J., Jungmann, F., Steinborn, M., Saleh, A., Makowski, M., Rueckert, D., & Braren, R. (2021). End-to-end privacy preserving deep learning on multi-institutional medical imaging. Nature Machine Intelligence, 3, 473 - 484.
[4] Khalifa, M., & Albadawy, M. (2024). AI in Diagnostic Imaging: Revolutionising Accuracy and Efficiency. Computer Methods and Programs in Biomedicine Update.
[5] Chen, Z., Lou, Y., Wang, B., Lei, H., & Yang, P. (2024). Application of Cloud-Driven Intelligent Medical Imaging Analysis in Disease Detection. Journal of Theory and Practice of Engineering Science.
[6] Holub, P., Müller, H., Bíl, T., Pireddu, L., Plass, M., Prasser, F., Schlünder, I., Zatloukal, K., Nenutil, R., & Brázdil, T. (2022). Privacy risks of whole-slide image sharing in digital pathology. Nature Communications, 14.
[7] S, G., & S, G. (2023). Securing medical image privacy in cloud using deep learning network. Journal of Cloud Computing, 12, 1-15.
[8] Kaissis, G., Makowski, M., Rückert, D., & Braren, R. (2020). Secure, privacy-preserving and federated machine learning in medical imaging. Nature Machine Intelligence, 2, 305 - 311.
[9] Chen, Y., & Esmaeilzadeh, P. (2024). Generative AI in Medical Practice: In-Depth Exploration of Privacy and Security Challenges. Journal of Medical Internet Research, 26.