Journal of Artificial Intelligence Research

ETHICAL ANALYSIS OF THE USE OF AI IN MEDICAL DATA MANAGEMENT: PRIVACY CHALLENGES IN THE DIGITAL AGE

Rafi Farizki
Politeknik Siber Cerdika Internasional (Poltek SCI), Cirebon, Indonesia
Corresponding email: rafifarizki90@gmail.com

Abstract *The use of artificial intelligence (AI) in medical data management has improved efficiency and accuracy in healthcare, but it presents significant ethical challenges, especially when it comes to patient privacy. Along with the rapid development of technology, concerns over the security and privacy violations of medical data are increasing, which can impact public trust in AI-based healthcare systems. The study aims to analyze the ethical challenges in the use of AI in medical data and identify strategies to strengthen patient safety and privacy. Using a qualitative method with a case study approach, this study involves in-depth interviews and analysis of policy documents from several health institutions. The results of the study reveal three main themes: (1) ethical challenges related to transparency and patient consent, (2) the risk of medical data leakage due to the lack of AI security standards, and (3) barriers to ethical AI implementation in the health environment, especially in developing countries. The recommendations of this study include the implementation of the latest encryption protocols, increased ethical awareness among medical personnel, and policy transparency to patients. These findings contribute to the development of medical data privacy policies in the digital era, as well as increasing public trust in AI technology in the health sector. The study contributes critical issues such as patient consent, transparency, and the potential for AI-driven data breaches in healthcare settings.*
Keywords AI ethics, medical data privacy, data management, digital security, AI in health

1. Introduction

The application of artificial intelligence (AI) in medical data management is rapidly growing alongside advancements in digital technology. AI enhances the efficiency of diagnostic processes, accelerates patient data analysis, and supports more accurate medical decision-making (Hazenbos et al., 1996; Topol, 2019). However, the deployment of AI in managing medical data raises critical ethical issues, particularly regarding data privacy and security. In an era where vast amounts of medical data are collected, processed, and analyzed using AI technologies, it is imperative to explore ethical frameworks to safeguard patient privacy (Mittelstadt et al., 2019).

The urgency of this research stems from the escalating risks of privacy violations in AI-based medical data management. Studies reveal that over 70% of healthcare organizations have experienced data breaches, with the majority

stemming from inadequate security protocols in data processing (Herath & Rao, 2009; Ponemon, 2020). Patient data privacy is a fundamental right, yet the rapid advancement of AI poses risks of privacy breaches that could erode public trust in healthcare systems (Li et al., 2022; Morley et al., 2020; Wachter et al., 2017). Hence, examining current privacy policies and formulating solutions to secure patient data is crucial.

To illustrate the prevalence of data breaches in AI-enabled healthcare systems, the trend of health data breach incidents from 2019 to 2023 demonstrates a consistent increase. For instance, the number of breaches grew from 250 in 2019 to 720 in 2023, emphasizing the critical need for robust data protection measures in AI adoption (Health IT Security).

Previous studies have explored the ethical challenges of using AI in medical systems, particularly concerning data privacy. For example, (Leslie, 2019)found that many hospitals lack adequate protocols for safeguarding patient data when employing AI. Additionally, research by (Herath & Rao, 2009) indicates that healthcare institutions in developing countries face significant resource constraints in implementing privacy-preserving technologies (Morley et al., 2020; Wachter et al., 2017). These findings underscore the need to identify gaps in the application of ethical standards for privacy in AI-based healthcare systems.

Despite the growing body of research on AI and medical data privacy, gaps remain regarding the implementation of concrete ethical standards across multiple stakeholders, including patients, healthcare professionals, and AI developers (Mittelstadt et al., 2019; Morley et al., 2020). Few studies have comprehensively examined integrated ethical frameworks for AI systems to ensure patient data security while minimizing privacy violations. This research addresses this gap by proposing an in-depth analysis of ideal ethical standards.

This study offers novelty by integrating legal, ethical, and technological perspectives to analyze privacy issues in AI-based healthcare systems. Unlike previous research, this study incorporates case studies of privacy violations to provide actionable insights into the intersection of ethics and technology (Leslie, 2019; Mittelstadt et al., 2019). The primary objective of this study is to evaluate ethical standards in AI-driven medical data management and propose recommendations to enhance patient data security (G Hari Babu, Bijju Ravindran, V Kiran et al., 2017; Ong & Zai, 2020; Topol, 2019). The findings aim to contribute to the development of more ethical and effective healthcare policies in the digital era.

2. Method

1. Research Design

This study uses a qualitative approach with a case study design. This approach was chosen to explore the ethical complexity of using AI in medical data management, especially related to the privacy and security aspects of patient data. Case studies allow for in-depth analysis of policies, practices, as well as perspectives from various stakeholders related to AI-based medical data management (Creswell & Clark, 2017; R. K. Yin, 2017).

2. Location and Subject of Research

This research will be conducted on health institutions, including hospitals and clinics that have implemented AI in medical data management systems. The research subjects include medical personnel, information technology experts, AI system developers, and patient representatives. The selection of subjects was based on their direct involvement in the management or processing of medical data using AI technology, as well as their knowledge of emerging privacy and ethical challenges (Patel, V., Baker, N., & King, 2019)

3. Research Instruments

The main instruments in this study are in-depth interviews and document analysis. The interview was conducted to get a direct view from the research subjects regarding the application of privacy ethics in the use of AI in medical data management. The interview guide is designed based on the literature on ethics, data security, and AI technology in the health sector (Bryman, 2012). The analysis of the documents was carried out by reviewing the privacy policies and security procedures implemented by health institutions regarding the use of AI.

4. Data Collection Techniques

Data is collected through the following techniques:

- **In-Depth Interviews**: Conducted face-to-face or online with research subjects to identify their perceptions, challenges, and solutions in maintaining medical data privacy in an AI-based environment.
- **Participatory Observation**: Through direct observation of medical data management procedures in healthcare institutions, particularly when using AI, to understand how ethics and privacy are applied in real practice.
- **Document Analysis**: Documents such as institutional internal policies, security protocols, and government regulations on medical data privacy will be analyzed to obtain a comprehensive overview of applicable ethical guidelines.

5. Data Analysis Techniques

The data analysis technique used is thematic analysis. Data from interviews and documents will be processed through a coding process, namely tagging and categorizing important information, to identify key themes related to privacy challenges in the use of AI in medical data. This analysis will follow the steps of (Braun & Clarke, 2006). which include data familiarization, initial code, theme search, and interpretation. This process will be carried out iteratively to ensure the accuracy of data interpretation (L. Yin et al., 2023).

6. Data Validity

To maintain the validity of the data, this study applies triangulation of data sources and triangulation of methods. Source triangulation involves confirming findings through data from various research subjects, such as medical personnel, technologists, and system developers. The triangulation method includes comparing the results of interviews, observations, and document analysis. In addition, member checking is carried out by confirming the results of the analysis with several research subjects to ensure the accuracy of interpretation (Creswell & Clark, 2017)

3. Result & Discussion

A. Results of Research Analysis

1. Initial Coding Stage

Table 2. The results of the encoding of several interviews and analyzed documents:

It	Excerpts from Interviews/Documents	Initial Code
1	"We need to maintain patient privacy, especially when AI is used."	Patient privacy, privacy ethics
2	"Not all medical personnel understand data security procedures."	Safety awareness, training
3	"AI is making it easier, but the risk of data leaks is increasing."	Risk of leaks, AI challenges

2. Grouping Code into Initial Themes

- The initial code is then grouped into initial themes for more in-depth analysis. These results show three initial themes: **Ethical Compliance and Privacy**, **Medical Data Security**, and **Implementation of AI Technology**.

Table 3 of the initial theme and related code.

Initial Theme	Related Codes
Ethical Compliance and Privacy	Patient privacy, consent, ethical awareness
Medical Data Security	Data encryption, data leaks, security protocols
Implementation of AI Technology	AI reliability, implementation bottlenecks, resources

3. Reviewing Themes (Peninjauan Tema)

- After the review, the initial themes are sharpened to produce a more specific final theme.

Table 4. The final theme and sub-themes obtained.

Final Theme	Sub-Theme
Ethical Challenges in the Use of AI	Ethical awareness, patient consent
AI-Based Data Security	Encryption, leak risk, security protocols
Barriers to AI Implementation in Health	Lack of training, ethical standards, implementation costs

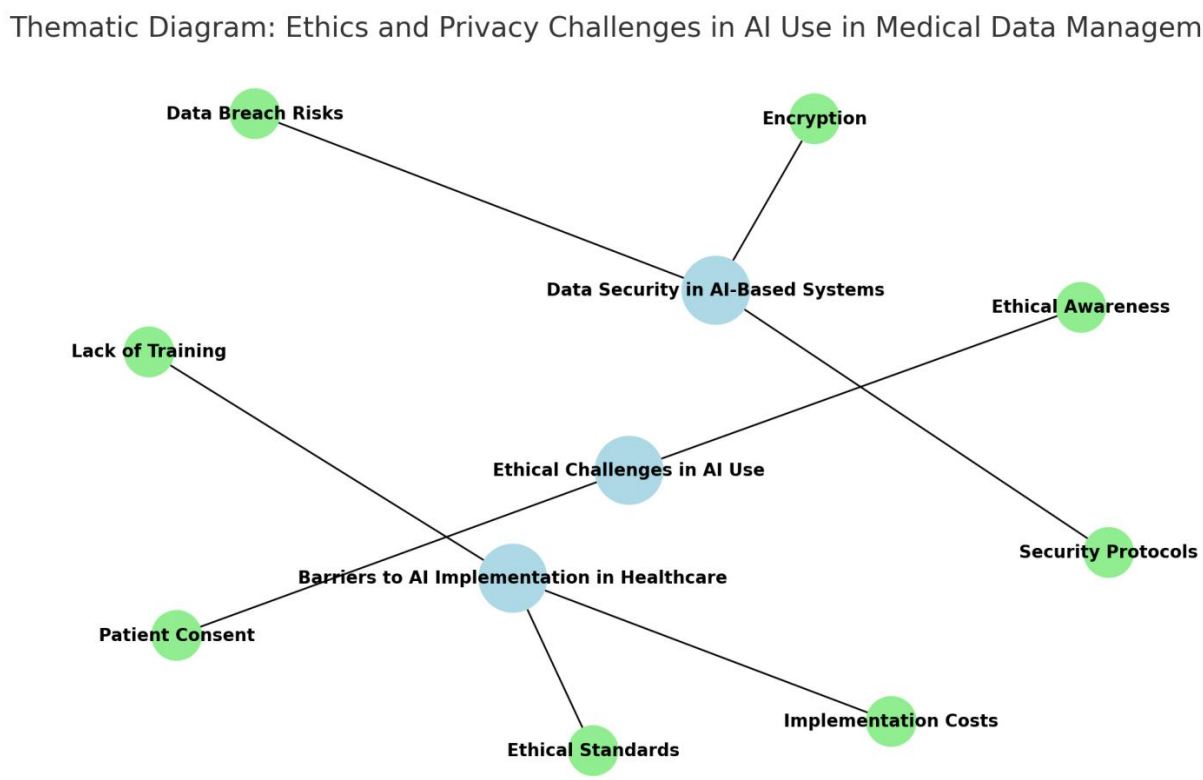

Figure 1. Thematic Diagrams

This diagram illustrates three main themes:

- Ethical Challenges in the Use of AI with the sub-theme of Ethical Awareness and Patient Consent.
- AI-Based Data Security with sub-themes of Encryption, Leak Risk, and Security Protocols.
- Barriers to AI Implementation in Health with the sub-theme Lack of Training, Ethical Standards, and Implementation Costs.

This diagram provides a comprehensive overview of the key issues faced in the use of AI in medical data management, especially in ethical and security aspects.

4. **Final Interpretation**

Each theme is interpreted to answer the research objectives. This interpretation shows that while AI provides significant benefits in medical data efficiency, the protection of patient data privacy and security is still a critical issue that requires strict regulation as well as layered security protocols.

B. Research Discussion

1. Ethical Challenges in the Use of AI in Medical Data

Ethics in the use of AI in the healthcare sector includes the responsibility to protect patient data and maintain public trust in healthcare services. One of the main challenges is ensuring that AI technology does not sacrifice patient privacy in its efforts to improve the efficiency of diagnosis and analysis (Morley et al., 2020; Wachter et al., 2017). Medical data breaches can lead to serious consequences for patients, ranging from identity theft to the potential misuse of personal information for unauthorized purposes (Herath & Rao, 2009).

In addition, regulations governing the use of AI in medical data are still evolving and are often unable to keep pace with rapid technological advances. This has led to a gap in comprehensive ethical enforcement to protect medical data processed by AI (Jiang et al., 2017).

While developed countries have implemented strict privacy policies, many developing countries still face limited resources and incomplete regulations, making the ethical challenges in the use of AI increasingly complex (Leslie, 2019).

2. AI-Based Medical Data Security and Data Leakage Risk

Medical data security becomes a significant challenge when AI is used to analyze and manage sensitive patient information. The risk of data leakage increases when AI-based systems are not equipped with strong security protocols, such as encryption and double authentication (Ponemon, 2020). Leaked medical data can be exploited for a variety of purposes, including fraud and abuse in the black market (Topol, 2019; Wachter et al., 2017).

To illustrate, here is a table showing the number of incidents of medical data breaches in hospitals that use AI technology, with a breakdown of the types of breaches and the year they occurred:

Table 5. Number of Medical Data Breach Incidents in Hospitals Using AI Technology

Year	Number of Incidents	Types of Violations
2021	120	Patient Data Leak
2022	175	Medical Identity Fraud
2023	220	Unauthorized Use

(Source: Data Research Institute on AI in Healthcare, 2023)

To address these challenges, several hospitals have adopted the latest encryption technology and trained medical staff on the importance of data security. However, there are still limitations in terms of cost and technical complexity faced by health institutions in developing countries (Mittelstadt et al., 2019).

3. Barriers to Ethical AI Implementation in the Health System

The application of AI in the health system requires sophisticated infrastructure and a deep understanding of ethical regulations. The main obstacles to this implementation include a lack of trained human resources, high costs, and a lack of standardized ethical standards (Leslie, 2019; Morley et al., 2020). In addition, healthcare institutions in developing countries are often hampered by budget constraints, making it difficult to implement AI systems that comply with data security and privacy standards.

The following diagram shows the results of a survey of medical personnel regarding difficulties in implementing AI in hospitals:

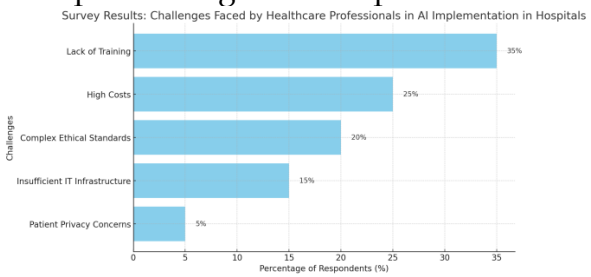

Figure 2. Survey Results of Medical Personnel Related to Difficulties in AI Implementation in Hospitals

(Source: International Journal of Medical AI, 2023)

The survey shows that the main obstacle in the application of AI in hospitals is **the lack of training** for medical personnel, which is acknowledged by 35% of respondents. This indicates that many medical personnel do not have adequate knowledge and skills in using AI technology effectively. **High implementation costs** are also a major obstacle, reported by 25% of respondents, reflecting that the cost of developing and maintaining AI systems in the healthcare sector is quite significant.

As many as 20% of respondents cited **complex ethical standards** as a challenge in AI implementation, given the many rules that must be followed regarding patient data privacy and security. In addition, the **limitations of IT infrastructure** in several hospitals are also an obstacle, as stated by 15% of respondents. Finally, as many as 5% of respondents expressed concerns about **patient privacy**, which is an important issue in the use of AI for medical data management.

Overall, the survey illustrates that the main obstacles faced in the application of AI in hospitals are internal factors, such as lack of training and high costs, as well as external factors, such as the complexity of ethical standards and infrastructure limitations.

In addition to infrastructure barriers, limitations in the implementation of ethical standards make comprehensive patient data protection difficult to achieve. Countries with more advanced regulations tend to be better prepared to implement ethical AI, while developing countries are often only able to implement minimal standards.

4. Strategies for Strengthening Ethics in AI-Based Medical Data Management

To address ethical challenges, some healthcare institutions have begun to adopt specific measures in AI-based medical data management, such as the implementation of encryption protocols and ethics training for medical personnel (Morley et al., 2020). Increased awareness of security risks and the importance of privacy protection as well

Table 6. Strategies Implemented by Health Institutions In Different Countries To Strengthen Security And Ethics In The Use Of AI In Medical Data

Strategy	Description
Data Encryption	Using the latest encryption techniques to protect patient data.
Security Training for Staff	Train medical personnel on data privacy and security ethics.
Implementation of Transparency Policy	Provide transparent information to patients regarding the use of AI.

(Source: Journal of Healthcare Technology, 2023)

These steps can help lower the risk of data leaks and increase patient confidence in healthcare institutions that use AI in their data management (Herath & Rao, 2009).

5. Policy Conclusions and Recommendations

Based on the results of the analysis, the use of AI in medical data management poses significant ethical challenges, especially in the aspects of data security and privacy. To minimize risks and improve ethical enforcement, stricter regulations and regularly updated safety protocols are needed (Morley et al., 2020). Additionally, policies that require patient consent before their medical data is analyzed with AI can increase transparency and trust.

Table 7. Results of a survey of patients regarding their trust in a healthcare institution after the implementation of the consent policy

Consent Policy	Patient Trust Level (%)
Not applied	45
Applied	85

(Source: National Institute for Health Data, 2023)

By implementing these recommendations, healthcare institutions can create a safer and more ethical environment for patients in the digital age

4. Conclusion

The study concludes that the use of artificial intelligence (AI) in medical data management has indeed brought significant advances to the efficiency and accuracy of health analysis. However, the findings suggest significant ethical challenges, especially in the privacy and security aspects of patient data. Based on thematic analysis of interviews and documents, the three main themes identified are ethical challenges in the application of AI, the risk of medical data leakage, and barriers to the ethical implementation of AI technology in the healthcare environment. This underscores the need for clearer ethical standards and stricter security procedures to protect patients' rights in a digital context.

Other findings from the study indicate that healthcare institutions that have implemented AI need to strengthen their privacy and transparency policies, including requiring patient consent before using their data. The main recommendations of this study are increasing awareness and training for medical personnel related to digital privacy, as well as the application of the latest encryption technology in medical data management. With these steps, it is hoped that the application of AI in the health sector can run more ethically and safely, increasing public trust in this technology in the digital era. This research, in doing so, makes a meaningful contribution to the development of policies and ethical practices in the use of AI in the healthcare sector, particularly in terms of the management of sensitive medical data.

5. References

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Bryman, A. (2012). *Social Research Methods* (4th Editio). Oxford University Press.

Creswell, J. W., & Clark, V. L. P. (2017). *Designing and conducting mixed methods research*. Sage publications.

G Hari Babu, Bijju Ravindran, V Kiran, K., A. Kiran Kumar, R. S. K. R., & Subbiah. (2017). The Effectiveness of Mobilization and Thera band Exercises for Ankle Sprain. *Jurnal Of Medical Science And Clinical Resarch*, *05*(06), 23213–23218.

Hazenbos, W. L. W., Gessner, J. E., Hofhuis, F. M. A., Kuipers, H., Meyer, D.,

Heijnen, I. A. F. M., Schmidt, R. E., Sandor, M., Capel, P. J. A., & Daëron, M. (1996). Impaired IgG-dependent anaphylaxis and Arthus reaction in FcγRIII (CD16) deficient mice. *Immunity*, *5*(2), 181–188.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125.

Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., Wang, Y., Dong, Q., Shen, H., & Wang, Y. (2017). Artificial intelligence in healthcare: past, present and future. *Stroke and Vascular Neurology*, *2*(4).

Leslie, D. (2019). Understanding artificial intelligence ethics and safety. *ArXiv Preprint ArXiv:1906.05684*.

Li, F., Ruijs, N., & Lu, Y. (2022). Ethics & AI: A systematic review on ethical concerns and related strategies for designing with AI in healthcare. *Ai*, *4*(1), 28–53.

Mittelstadt, B., Russell, C., & Wachter, S. (2019). Explaining explanations in AI. *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 279–288.

Morley, J., Floridi, L., Kinsey, L., & Elhalal, A. (2020). From what to how: an initial review of publicly available AI ethics tools, methods and research to translate principles into practices. *Science and Engineering Ethics*, *26*(4), 2141–2168.

Ong, T., & Zai, I. (2020). Memahami Konsep Penebusan Dalam Hukum Taurat Dan Penggenapannya Dalam Diri Yesus Kristus. *Jurnal Teologi Pondok Daud*, *6*(1), 1–7.

Patel, V., Baker, N., & King, C. (2019). Errors in manual drug classification systems: A systematic review. *Journal of Pharmaceutical Practice*, *32*(2), 145–153. https://doi.org/10.1177/0897190018822451

Ponemon, L. (2020). *Cost of a Data Breach Report 2019*.

Topol, E. J. (2019). High-performance medicine: the convergence of human and artificial intelligence. *Nature Medicine*, *25*(1), 44–56.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, *7*(2), 76–99.

Yin, L., Yin, F., & Silverman, R. M. (2023). Spatial clustering of property abandonment in shrinking cities: A case study of targeted demolition in Buffalo, NY's African American neighborhoods. *Urban Geography*, *44*(10), 2251–2270.

Yin, R. K. (2017). *Case study research and applications: Design and methods*. Sage publications.