IJSSR
International Journal of Social Service and Research

Vol. 4, No. 11, November 2024
e-ISSN: 2807-8691 | *p*-ISSN: 2807-839X

PATIENT DATA PROTECTION IN THE DIGITAL ERA (CHALLENGES AND LEGAL SOLUTIONS)

Ineke Winda Ferianasari
Universitas Borobudur, Indonesia
*e-mail: inekewfs@gmail.com

Keywords
Artificial Intelligence, Digital Age, Patient Data Protection,

ABSTRACT

Artificial intelligence (AI) has emerged as a promising technology in the field of healthcare, enabling the development of innovative solutions that enhance the quality and efficiency of medical services. The application of AI in the management of patient data has facilitated the acceleration, optimization, and precision of this process, which can subsequently improve the quality of healthcare services. This study aims to analyse the legal challenges that arise with the use of digital technology and artificial intelligence in patient data management, and to identify relevant legal solutions to overcome these problems. The study employs library research techniques, analysing statutory provisions and drawing on both written and unwritten positive law to examine legal issues. The results show that the integration of AI and digital technology in healthcare has yielded significant advantages, including enhanced efficiency, precision in diagnosis, and the harnessing of big data for patient care. However, a number of significant challenges remain, particularly with regard to the safeguarding of personal data. The formulation of an ethical framework for the utilisation of AI, the establishment of rigorous safety standards and the continuation of research in this domain are vital to enhance the advantages and mitigate the risks associated with the deployment of AI. It is imperative that health institutions and AI developers implement robust cybersecurity standards and periodic assessments for potential system vulnerabilities.

INTRODUCTION

The development of technology that runs so fast causes the emergence of cutting-edge technologies that are increasingly developed, one of which is artificial intelligence (AI). Artificial intelligence (AI) is a technology that can think like humans but is run by robots not naturally from humans themselves. In general, Artificial intelligence (AI) uses a certain level of intelligence that can perform human-like functions such as perception, knowledge and creativity (Arly et al., 2023). Artificial intelligence is a computer system capable of performing tasks that would normally require human intelligence. This technology can make decisions by analysing and using data available in the system. The process that occurs in Artificial intelligence includes learning, reasoning, and self-correction. This process is similar to humans analysing before making a decision. Artificial intelligence (AI) is one of the innovations in the industrial revolution era (Lubis, 2021).

The development of digital technology has changed many aspects of human life, including in the field of health (Nugroho et al., 2023). Information technology and artificial intelligence (AI) have become integral to the management of medical data, whether in the context of electronic medical record storage, health data processing, or the delivery of data-driven health services (Prasanti & Indriani, 2018). The implementation of AI in patient data management facilitates the acceleration, optimization, and precision of this process, which can subsequently enhance the quality of healthcare services. However, these advancements do not come without challenges, particularly with regard to the protection of

personal data and the safeguarding of patient privacy rights (Suhartono & Assyfa, 2023). Artificial intelligence (AI) is defined by its capacity to comprehend and execute actions that are most likely to attain a desired outcome. Artificial intelligence (AI) is regarded as the driving force behind the fourth industrial revolution, and it has now reached the stage of AI disruption. (Hadi & Guntara, 2022).

In the field of healthcare, medical records are deeply intertwined with the day-to-day activities of healthcare professionals. This has led to the observation that medical colleagues can be considered a third party when doctors receive patients. This can be understood by considering that medical records are records of examinations and actions related to the handling of patients by doctors. Medical records are defined as files that contain records and documents pertaining to a patient's identity, medical examination, treatment, actions, and other services provided to the patient. Medical records are a compilation of data pertaining to the identity of the patient, the results of the anamnesis, the findings of the examination, and the documentation of all activities undertaken by healthcare providers for the benefit of the patient (Giyana, 2012).

Medical records are written and recorded information about a patient's identity, medical history, physical examination, laboratory and radiology test results, diagnosis, and all medical services and actions provided to the patient, including outpatient, inpatient, and emergency services (Handiwidjojo, 2009). As stated by the Ministry of Health, medical records serve as a crucial metric for evaluating the quality of medical services rendered by hospitals and their respective medical personnel (Kurniawan & Setiawan, 2021). One of the parameters for determining the quality of health services in hospitals is data or information derived from comprehensive and accurate medical records. The quality of medical records can be assessed based on several criteria, including the completeness of the content, accuracy, timeliness, and compliance with legal requirements. In the event of an error in the recording of information in medical records, it is imperative that the relevant files and records are not removed or deleted in any way (Bintariyati et al., 2022).

Patient data represents a category of sensitive information that, if disclosed or exploited inappropriately, can give rise to a range of adverse consequences. These may include infringements of privacy or the potential for identity fraud (Priscyllia, 2019). In the context of the digital age, the risk of data leakage is becoming increasingly intricate and frequently challenging to foresee. Data leakage can be defined as the disclosure of confidential information, whether inadvertent or intentional, to unauthorized parties (Long et al., 2017). The utilisation of AI technology for the processing of vast quantities of data presents a novel avenue for the potential exploitation of such data, whether by unauthorised third parties or through the deployment of increasingly sophisticated cyberattacks. It is therefore imperative that patient data protection be accorded the serious attention it deserves (Disemadi, 2021). In the rule of law in Indonesia, every criminal offense, whether it involves a crime or a violation, must still be processed under the existing laws (Hernanto & Amelia, 2024)

Article 297 of Law Number 17 of 2023 on Health (the "Law on Health") specifically regulates the confidentiality, integrity, security, and availability of data in medical record documents, imposing an obligation on health service facilities to maintain these standards. A comparable issue is addressed in Minister of Health Regulation Number 24 of 2022 concerning Medical Records, Article 32, which stipulates that all individuals involved in health services at healthcare facilities are obliged to maintain the confidentiality of the contents of medical records, even in the event of the patient's demise. Moreover, Regulation of the Minister of Health Number 36 of 2012 concerning Medical Secrets, Article 4, also addresses this issue. It stipulates that all individuals involved in medical services and/or utilizing data and information about patients are obliged to maintain the confidentiality of medical secrets (Hadi & Guntara, 2022).

As technology continues to advance, it is imperative that concrete steps be taken by a variety of stakeholders, including regulators, healthcare providers, and technology developers, to collaborate in the creation of a secure ecosystem for the protection of patient data. The success of patient data protection is contingent upon the establishment of rigorous regulatory frameworks and the fostering of mutual awareness and responsibility among stakeholders with regard to the maintenance of data security and confidentiality in the context of the ongoing digital revolution. It is also incumbent upon technology developers to create solutions that are not only effective but also ethical. It is imperative that the technologies developed are subjected to rigorous security and privacy standards, and that the social impact of the technology applications is duly considered. Through collaborative efforts, all stakeholders can collectively foster public trust in the digital health system, which in turn will facilitate the broader adoption of health technology.

It is of significant importance to educate the general public about their rights regarding personal data and the means by which they can safeguard their information. A greater public awareness of privacy issues may result in an increased demand for more transparent and responsible practices in the management of health data. It is anticipated that the implementation of a holistic and collaborative approach will facilitate the effective protection of patient data, thereby encouraging innovation and improving the quality of health services in the context of an increasingly digital era.

The purpose of this study is to analyse the legal challenges that arise with the use of digital technology and artificial intelligence in patient data management, and to identify relevant legal solutions to overcome these problems. This study contributes to the intersection of law, healthcare, and digital technology by addressing the legal challenges associated with using artificial intelligence and digital technology in patient data management. It provides practical legal solutions to guide policymakers and healthcare administrators in developing robust regulatory frameworks that ensure data security, ethical practices, and compliance with legal standards. The research promotes a balanced approach to safeguarding patient rights while fostering innovation, supporting institutions in aligning with regulations, and enhancing trust among stakeholders. Additionally, it lays a foundation for future studies on the legal implications of AI in healthcare, contributing to the broader discourse on ethical and secure data usage.

METHODS

The research adopts a normative juridical approach, focusing on the analysis of legal principles and frameworks to address challenges and propose solutions regarding the utilisation of artificial intelligence in patient data management within the digital age. This method involves a comprehensive examination of primary legal materials, including Law No. 17 of 2023 on Health, Regulation of the Minister of Health No. 36 of 2012 on Medical Secrets, and Regulation of the Minister of Health No. 24 of 2022 on Medical Records, alongside secondary legal materials such as legal doctrines, academic literature, and scientific articles.

The research procedure includes identifying and collecting relevant legal documents and regulations, followed by a qualitative analysis that associates the data with pertinent legal provisions and principles. The study employs library research techniques, analysing statutory provisions and drawing on both written and unwritten positive law to examine legal issues. This approach provides a robust foundation for understanding and addressing the legal complexities surrounding AI-driven patient data management.

RESULTS

The Utilization of Digital Technology and Artificial Intelligence in the Management of Patient Data Has Given Rise to A Number of Legal Challenges

The integration of digital technology and artificial intelligence (AI) in healthcare has yielded significant advantages, including enhanced efficiency, precision in diagnosis, and the harnessing of big data for patient care. Nevertheless, the implementation of these technologies also gives rise to a number of legal issues that must be addressed in order to safeguard patient rights and maintain the integrity of the healthcare system.

The application of artificial intelligence (AI) in the gathering and examination of personal data gives rise to significant concerns pertaining to individual privacy (Dwork et al., 2016). One of the principal reasons why the utilisation of AI can potentially infringe upon individual privacy is due to its capacity to discern patterns within personal data. Artificial intelligence algorithms are capable of analysing data with a degree of precision and velocity that traditional methodologies are unable to attain. However, it is possible that sensitive information contained in personal data may be revealed without the consent or knowledge of the individuals concerned during this process (Siti Masrichah, 2023).

The use of Artificial intelligence (AI) in the face of AI threats and opportunities is inseparable from the technical, ethical, and security challenges that need to be considered. In recent years, various studies have identified several aspects that need to be considered in the responsible use of AI. Here are some of the key challenges to consider (Morgan et al., 2020):

1) Technical Challenges: The technical challenges associated with AI include the collection and processing of quality data, the reliability and accuracy of algorithms, and the availability of sufficient computing capacity. In order to achieve the greatest possible benefit from the use of

AI, it is essential that access is available to sufficient, relevant, and of a high quality. Additionally, the creation of dependable and precise algorithms is crucial for the attainment of accurate and reliable outcomes. Moreover, AI necessitates the provision of adequate computing resources, including sufficient processing speed and storage capacity to accommodate the execution of extensive and intricate tasks.

2) Ethical Challenges: The application of AI also gives rise to a number of significant ethical concerns. One of the most significant challenges is ensuring fairness and eliminating bias. It is possible that AI algorithms may reflect biases present in the training data or apply unfair decisions. It is therefore imperative that AI algorithms are developed and implemented in accordance with the principles of fairness, equality, and non-discrimination. Furthermore, ethical considerations extend to the domain of privacy and the protection of personal data. In the context of the collection and analysis of sensitive data, such as medical or financial data, it is of paramount importance to maintain the confidentiality of individual information and to guarantee the security of the data in question.
3) Security Challenges: Furthermore, the utilisation of AI gives rise to a number of security concerns that must be addressed. Artificial intelligence (AI) systems are susceptible to exploitation and manipulation, whether through cyberattacks or data manipulation. It is of the utmost importance to prioritize the security of AI systems in the development and deployment of this technology. It is imperative that robust measures be implemented to safeguard AI systems from potential security threats. This entails the implementation of comprehensive data protection measures, the fortification of computing infrastructure, and the conduct of rigorous security testing.

In order to effectively address these challenges, it is essential to adopt a comprehensive approach that engages the expertise of relevant professionals, including researchers, regulators, and practitioners. The formulation of an ethical framework for the utilisation of AI, the establishment of rigorous safety standards, and the continuation of research in this domain are vital to enhance the advantages and mitigate the risks associated with the deployment of AI. With regard to the challenges of artificial intelligence in patient data management, several challenges emerge with regard to the implementation of AI-based health services. These include aspects of effectiveness and security, responsibility, data protection, personal data protection, cybersecurity, and aspects of copyright law (Siregar, 2023).

The confidentiality of patient data is a crucial element in the relationship between doctors and patients. This is contingent upon the ability to organize data-based health services and AI, which will require a substantial and diverse array of data about patients that is both personal and sensitive in nature (Trenggono & Bachtiar, 2023). As the data steward, the patient must grant permission for their personal data and medical records to be accessed by the information system in order for the latter to be able to process the data further and provide the most suitable recommendations. Information on the purpose and scope of data utilization should be provided, including the identity of the data recipients and the nature of the data to be disclosed. It is the responsibility of the organizer to ensure that the patient's data is managed in an appropriate manner and that it is not disseminated or used for other purposes without the patient's knowledge. The term "data management as intended" encompasses the utilization, storage, access, and dissemination of data, including for research, publication, and other purposes (Librianty & Prawiroharjo, 2023).

The Personal Data Protection Law, for example, is often lacking in specificity with regard to the regulation of the use of technologies such as AI in the healthcare system, which has resulted in the emergence of regulatory gaps. A further challenge is that of transparency in the context of AI-based decision-making. The opacity of many AI algorithms, even to their developers, introduces a risk of unclear liability in the event of misdiagnosis or inappropriate medical treatment (Prastiwi et al., 2023). Furthermore, the potential for bias in AI algorithms represents a significant challenge. If AI is trained with non-representative data, there is a risk of biased decisions, which may result in discriminatory outcomes for specific patient groups (Ramadhani, 2024).

From an ethical standpoint, questions also emerge concerning the extent to which AI can or should assume responsibilities that were previously the exclusive domain of human medical personnel, as well as the accountability of decisions made by AI in a clinical context. Patients may lack sufficient understanding of how their data is being utilized, particularly for technological development purposes. Therefore, it is imperative to implement more transparent and comprehensive regulation of patients'

rights to their data (Indra et al., 2024). Furthermore, patient consent mechanisms frequently prove inadequate due to the intricate nature of the technology, which is challenging to elucidate in a readily comprehensible manner. In sum, these legal challenges demand a comprehensive approach that entails updating regulations, establishing more rigorous standards for AI-based health data management, and enhancing awareness of all stakeholders regarding their rights and responsibilities. In the formulation of policies aimed at maintaining a balance between technological innovation and the protection of patients' rights, data security, transparency in decision-making, and the ethical use of technology should be accorded the highest priority.

Relevant legal Solutions to Overcome Problems with the Use of Digital Technology and Artificial Intelligence in Patient Data Management

The application of artificial intelligence (AI) in the field of healthcare has facilitated the development of innovative solutions that enhance the quality of medical services. The capacity of AI to rapidly and accurately analyse vast quantities of data enables medical professionals to gain more profound insights in a shorter time frame (Kementrian Kesehatan, 2024). The process of diagnosis, treatment planning, and early detection of diseases that previously required a lengthy time frame can now be expedited with the assistance of AI. This not only enhances efficiency but can also prove lifesaving by facilitating more prompt and precise medical interventions. Other advantages offered by AI include the personalization of care, whereby in-depth data analysis enables the provision of care that is more tailored to the specific needs of each patient, based on their health profile.

Nevertheless, despite the considerable advantages conferred by AI in the field of healthcare, a number of significant challenges remain, particularly with regard to the safeguarding of patient data. The confidentiality, security, and privacy of data are of paramount importance in the context of the deployment of AI in healthcare (Andika & Soemarno, 2023). It is of the utmost importance to safeguard patient data, which is of a highly sensitive and personal nature, from any form of misuse or exploitation. This is particularly true given the potential for such data to be misused if it falls into the hands of those who may not have the requisite level of responsibility or accountability. The leakage or manipulation of medical information has the potential to negatively impact a patient's personal life in a multitude of ways, including affecting their health, social interactions, and economic stability.

It is therefore evident that robust and comprehensive legal solutions are required to address these issues. It is essential that the law strikes a balance between the necessity to encourage technological innovation in healthcare and the obligation to protect patients' rights to privacy and security of their data (Simamora & Indah, 2022). Effective legal arrangements should include robust data protection mechanisms, rigorous security standards, and the right of patients to be fully informed about the use of their data, to exercise control over it, and to provide explicit consent for its processing. Concurrently, legal solutions must facilitate the advancement of the innovation ecosystem while ensuring the protection of patient privacy and security. In light of these considerations, the most appropriate legal solutions to address these issues are as follows:

1) Improvement of Patient Data Protection Regulations: The protection of patient data is a fundamental aspect that must be considered in the use of AI in healthcare. Data protection regulations, such as Law No. 27 of 2022 on Personal Data Protection (PDP) in Indonesia or the General Data Protection Regulation (GDPR) in the European Union, provide a legal framework that can be adapted to the use of AI in healthcare (Kusworo et al., 2022). In the context of artificial intelligence (AI), it is imperative that regulations pertaining to data collection, storage, and utilization be reinforced in order to ensure compliance with established privacy principles (Srigantiny et al., 2024). It is imperative that enforcement mechanisms be reinforced with respect to the safeguarding of personal data, particularly in light of the growing prevalence of digital technology and artificial intelligence (AI) in the domain of health data management. It is imperative that regulations encompass a multitude of aspects, including transparency, explicit consent, and patients' rights to access and control their data. Furthermore, it is imperative to motivate technology developers to integrate privacy principles from the system design stage onwards. This guarantees that data protection is incorporated into the fundamental design of any technology.
2) Transparency in Data Usage: It is imperative that the general public be aware of the transparency of all forms of news reporting on an event. This awareness is necessary to ensure the accuracy of information in the current era of openness. This demand creates a tenuous

distinction between individual privacy and the public interest (Prananda, 2020). One crucial solution is to enhance transparency regarding the utilization of patient data. It is imperative that healthcare institutions and AI providers be transparent about the intended use of data, the reasons for its use, and the parties responsible for its use. This transparency should be achieved through the implementation of an expanded informed consent process, whereby patients are provided with comprehensive information regarding the potential risks, benefits, and their right to object to the utilization of their data by AI technologies.

3) Ethical Regulation in Health AI Development: AI used to analyse health data must be built to strict ethical standards (Nyoman & Purnama, 2024). It is imperative that the Medical Ethics Council and the AI Supervisory Board collaborate to establish ethical guidelines that encompass the tenets of fairness, accountability, and non-discrimination. One potential avenue for addressing these concerns is through the establishment of legal solutions, such as codes of ethics or regulatory guidelines, that mandate AI developers to ensure that their AI systems do not introduce bias into medical decision-making processes. Such bias could have adverse effects on patients based on factors such as gender, race, or economic status (Librianty & Prawiroharjo, 2023).
4) Data Security Obligations: An additional legal avenue for addressing the concerns surrounding the use of AI in healthcare is to reinforce the obligations pertaining to the security of health data. This can be achieved by implementing robust cybersecurity measures to prevent the leakage or misuse of sensitive information. It is imperative that health institutions and AI developers implement robust cybersecurity standards, including data encryption, the use of secure servers, and periodic assessments for potential system vulnerabilities. (Raharja, 2024). Failure to protect data should be followed by significant legal sanctions to provide a deterrent effect.
5) Supervision and Legal Liability: To ensure effective law enforcement, there should be a clear oversight mechanism. The Data Protection Supervisory Authority and other independent agencies can be empowered to monitor the use of AI in the healthcare sector. In addition, if there is a violation of patients' privacy rights, AI developers and healthcare institutions should be held legally responsible, including the obligation to compensate affected patients (Sumitra et al., 2024).
6) Harmonization of International Regulations: The term "international regulatory harmonization" is used to describe the process of creating coherent and consistent global standards to protect data privacy in the context of digital technology and artificial intelligence (AI) for patient data management. This is of particular importance given that patient data frequently transcends national boundaries, and regulatory frameworks can vary considerably between countries. The objective of harmonization is to establish a level playing field between countries, enabling technology companies, including those developing AI, to adhere to a single set of universal principles, thus eliminating the necessity to tailor their operations to the specific requirements of each jurisdiction. For example, the General Data Protection Regulation (GDPR) in the European Union establishes rigorous privacy standards and serves as a model for other countries. However, it should be noted that countries such as the United States have different regulatory frameworks in place, including the Health Insurance Portability and Accountability Act (HIPAA) (Nabanan et al., 2023). Harmonization is important because without a unified regulatory approach, there is a risk of differing legal interpretations that could hinder technological innovation and secure data management.
7) Strengthening Patient Rights: In light of the growing reliance on digital technology and artificial intelligence (AI) in healthcare, it is imperative to prioritize the protection of patient data. It would be prudent for Indonesia to reinforce the Personal Data Protection Law, as exemplified by Law No. 27 of 2022, in order to guarantee that patients' medical data is not exploited inappropriately and safeguarded from unauthorized disclosure (Meher et al., 2023). It is also imperative that legal solutions be implemented to reinforce patients' rights with regard to their data. This encompasses the right of access, the right to rectification, the right to delete data, and the right to transfer data to another healthcare provider. Patients must be granted comprehensive control over their data, with readily accessible and intelligible procedures for exercising those rights.

CONCLUSION

Artificial intelligence (AI) in healthcare offers significant opportunities for improving medical care quality and efficiency. However, it also presents challenges in safeguarding patient data, including confidentiality, security, and privacy. Technical challenges include data processing quality, algorithm development, and computing capacity. Ethical issues involve fairness, privacy, and personal data protection. To overcome these, a comprehensive legal solution is needed, including data protection regulations, transparency, and ethical standards in AI development. The use of AI in healthcare will continue to expand, ensuring privacy and security while delivering benefits to society. Future research should focus on developing AI-specific legal frameworks, harmonizing international regulations, implementing ethical AI implementation, assessing data security technologies, establishing stakeholder collaboration models, integrating patient input into AI systems, and assessing AI's impact on healthcare equity.

REFERENCES

Andika, & Soemarno, M. (2023). Masalah Privasi dan Keamanan Data Pribadi pada Penerapan Kecerdasan Buatan. *INNOVATIVE: Journal Of Social Science Research*, *3*, 4917–4929.

Arly, A., Dwi, N., & Andin, R. (2023). *Implementasi Penggunaan Artificial Intelligence Dalam Proses Pembelajaran Mahasiswa Ilmu Komunikasi di Kelas A*. Seminar Nasional.

Bintariyati, K. T., Suarjana, N., & Ketut Sujana, I. (2022). Identifikasi Faktor-Faktor Yang Mempengaruhi Mutu Rekam Medis Pasien Rawat Inap Ruang Apel Rumah Sakit Umum Daerah Kabupaten Klungkung. *Jurnal Kesehatan Terpadu*, *6*(2), 55–63.

Disemadi. (2021). AI Shield: Protecting Business Data from Cybercrime. *Formosapublisher*, *2*(2), 272.

Dwork, C., Mcsherry, F., Nissim, K., & Smith, A. (2016). Calibrating Noise to Sensitivity in Private Data Analysis. *Journal of Privacy and Confidentiality*, *7*.

Giyana, F. (2012). Analisis Sistem Pengelolaan Rekam Medis Rawat Inap Rumah Sakit Umum Daerah Kota Semarang. *Jurnal Kesehatan Masyarakat Universitas Diponegoro*, *1*(2), 187.

Hadi, A., & Guntara, B. (2022). Pembaharuan Hukum Nasional Dalam Upaya Perlindungan Data Pribadi Di Era Distrupsi Kecerdasan Buatan (Artificial Intelligence). *Jurnal Hukum Mimbar Justitia*, *8*(1), 233. https://doi.org/10.35194/jhmj.v8i1.2426

Handiwidjojo, W. (2009). Perkembangan Teknologi Rekam Medis Elektronik Di Rumah Sakit. *Universitas Kristen Duta Wacana Yogyakarta*, *2*(1), 36–41.

Hernanto, T. S., & Amelia, T. (2024). *Omnibus Law penegak Hukum Di Indonesia*. PT. Kaya Imu Bermanfaat.

Indra, I., Dewi, T. N., & Wibowo, D. B. (2024). Perlindungan Kerahasiaan Data Pasien vs Kewajiban Membuka Akses Rekam Medis Elektronik. *Soepra*, *10*(1), 97–117. https://doi.org/10.24167/sjhk.v10i1.11542

Kementrian Kesehatan. (2024). *Artificial Intelligence (AI) dan Electronic Medical Record (EMR) Game Changer dalam Transformasi Digital Kedokteran*. Kementerian Kesehatan. https://lms.kemkes.go.id/courses/4f12d00e-8954-493c-831e-4a91320f8c95

Kurniawan, A. L., & Setiawan, A. (2021). Perlindungan Data Rekam Medis Sebagai Bentuk Perlindungan Data Pribadi Pasien Selama Pandemi Covid-19. *Jurnal Hukum Dan Pembangunan Ekonomi*, *9*(1), 95. https://doi.org/10.20961/hpe.v9i1.52586

Kusworo, D. L., Pratama, A. A., Fauzi, M. N. K., & Shafira, M. (2022). Conception of An Independent Surveillance Authority in the Effort to Protect Population Data. *Administrative and Environmental Law Review*, *3*(1), 9–24. https://doi.org/10.25041/aelr.v3i1.2530

Librianty, N., & Prawiroharjo, P. (2023). Tinjauan Etika penggunaan Artificial Intelegence di Kedokteran. *Jurnal Etika Kedokteran Indonesia*, *7*(1). https://doi.org/10.26880/jeki.v7i1.68

Long, C., Lu, F., & Yao, D. D. (2017). Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions: Enterprise Data Breach. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discover*, *1*(1).

Lubis, MSY. (2021). *Implementasi Artificial Intelligence Pada System Manufaktur Terpadu*. SEMNASTEK UISU.

Meher, C., Sidi, R., & Risdawati, I. (2023). Penggunaan Data Kesehatan Pribadi Dalam Era Big Data: Tantangan Hukum dan Kebijakan di Indonesia. *Jurnal Ners*, *7*(2), 864–870. https://doi.org/10.31004/jn.v7i2.16088

Morgan, F., Boudreaux, B., Lohn, A., Ashby, M., Curriden, C., Klima, K., & Grossman, D. (2020). Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World. In *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World* (Issue September 2021). https://doi.org/10.7249/rr3139-1

Nabanan, D., Saragih, D., Widyaningrum, Dirgayunita, Musiana., & Sanjaya, S. (2023). *Ilmu Kesehatan*. Yayasan Cendikia Mulia Mandiri.

Nugroho, R., Hidayat, M., Rianti, E. D. D., Mutiarahati, N. L. A. C., & Rosyid, A. F. (2023). Pemanfaatan Teknologi Digital dalam Pelayanan Kesehatan Publik: Sebuah Tinjauan Analisis Kebijakan. *Ministrate: Jurnal Birokrasi Dan Pemerintahan Daerah*, *5*(2), 277–285. https://doi.org/10.15575/jbpd.v5i2.28550

Nyoman, N., & Purnama, P. (2024). *Implikasi Hukum Terhadap Penggunaan Kecerdasan Buatan Dalam Diagnosis Dan Pengobatan Penyakit Dalam Sistem Kesehatan*. *4*, 17355–17364.

Prananda, R. R. (2020). Batasan Hukum Keterbukaan Data Medis Pasien Pengidap Covid-19. *Law, Development & Justice Review*, *3*(1), 142–168.

Prasanti, D., & Indriani, S. S. (2018). Pengembangan Teknologi Informasi Dan Komunikasi Dalam Sitem E-Health Alodokter.com Com the Use of Information and Communication Technology in E-Health System Alodokter.Com. Jurnal Sosioteknologi,17(1),93103.http://journals.itb.ac.id/index.php/sostek/artic. *Jurnal Sosioteknologi*, *17*(1), 93–103.

Prastiwi, D., Lestari, W., Utami, R. T., Rinarto, N. D., Chabibah, N., Fitriyani, N. L., Amir., N. I., Irma, A., Juliantara, I. P. E., Sari, N. A., Nurfadillah, A., Suraduhita, A., & Ummu Syauqah Al Musyahadah. (2023). *Pengantar Biomedik Panduan Komprehensif* (Vol. 01).

Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. *Jatiswara*, *34*(3), 239–249. https://doi.org/10.29303/jtsw.v34i3.218

Raharja, A. R. (2024). *Keamanan Jaringan*. KBM Indonesia.

Ramadhani, Y. (2024). *AI Cerdas, tapi Bisa Bias? Waspada Bahaya Algoritma!* FTMM News.

Simamora, M. M., & Indah. (2022). Perlindungan Hukum Atas Hak Privasi Dan Kerahasiaan Identitas Penyakit Bagi Pasien Covid-19. *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan*, *1*(7), 1089–1098. https://doi.org/10.54443/sibatik.v1i7.126

Siregar, R. A. (2023). Perspektif Hukum tentang Transformasi PelayananKesehatan dengan Kecerdasan Buatan. *Jurnal Hukum Kesehatan*, *9*(2), 306–314. https://doi.org/. https://doi.org/10.24167/shk.v9i2.11270

Siti Masrichah. (2023). Ancaman Dan Peluang Artificial Intelligence (AI). *Khatulistiwa: Jurnal Pendidikan Dan Sosial Humaniora*, *3*(3), 83–101. https://doi.org/10.55606/khatulistiwa.v3i3.1860

Srigantiny, F., Brilian, Y., Jayanti, Y. E., SilitSrigantiny, F., Brilian, Y., Jayanti, Y. E., Silitonga, L., Santika, M., Prayuti, Y., & Lany, A. (2024). Pemenuhan Hak Pasien Atas Privasi dan Kerahasiaan Informasi Kesehatan di Rumah Sakit: Aspek Hukum Perdata. Penambahan Natrium Benzoat Dan Kalium , L., Santika, M., Prayuti, Y., & Lany, A. (2024). Pemenuhan Hak Pasien Atas Privasi dan Kerahasiaan Informasi Kesehatan di Rumah Sakit: Aspek Hukum Perdata. *Penambahan Natrium Benzoat Dan Kalium Sorbat (Antiinversi) Dan Kecepatan Pengadukan Sebagai Upaya Penghambatan Reaksi Inversi Pada Nira Tebu*, *10*(17), 404–411.

Suhartono, E., & Assyfa, A. Alifia. (2023). *Kecerdasan Buatan Dalam Bidang Kesehatan : Inovasi Dan Aplikasi*. ULM Press.

Sumitra, S., Prayuti, Y., & Lany, A. (2024). KEWAJIBAN DAN TANGGUNG JAWAB HUKUM PERDATA DALAM PERLINDUNGAN PRIVASI DATA PASIEN DALAM LAYANAN KESEHATAN DIGITAL. *Jurnal Hukum Media Justitia Nusantara*, *14*(1), 43–52.

Trenggono, P. H., & Bachtiar, A. (2023). Peran Artificial Intelligence Dalam Pelayanan Kesehatan : a Systematic Review. *Jurnal Ners*, *7*(1), 444–451. https://doi.org/10.31004/jn.v7i1.13612