JGSP
Jurnal Greenation Sosial dan Politik
+62 81210467572 https://greenationpublisher.org/JGSP greenation.info@gmail.com
GREENATION PUBLISHER

DOI: https://doi.org/10.38035/jgsp.v3i4

Evaluation of Changes in Patient Data Protection Regulations and Legal Obligations of Radiologists in The Era of Health Service Digitalization

Yuki Mulyani[1], Faisal Santiago[2]
[1]Universitas Borobudur, Jakarta, Indonesia, yukimulyani@yahoo.com
[2]Universitas Borobudur, Jakarta, Indonesia, faisalsantiago@borobudur.ac.id

Corresponding Author: yukimulyani@yahoo.com[1]

Abstract: The digital transformation in the healthcare sector has transformed the way patient data is managed, including in radiology, which now relies on electronic systems such as the Picture Archiving and Communication System (PACS). This change has created an urgent need for regulations capable of protecting medical data from potential leaks and misuse. This study aims to evaluate changes in patient data protection regulations and examine the legal obligations of radiologists in the era of digital healthcare services. The method used is normative juridical research with a statutory and conceptual approach, utilizing primary legal materials in the form of Law Number 27 of 2022 concerning Personal Data Protection and Law Number 17 of 2023 concerning Health, as well as secondary legal materials such as journals, books, and health law doctrine. The analysis shows that both laws have strengthened legal protection for patient data through stricter regulations regarding electronic medical records, data controller obligations, and sanctions for violations of personal data protection. However, the implementation of these regulations still faces technical and normative obstacles, including weak digital infrastructure, lack of legal literacy among medical personnel, and suboptimal inter-agency coordination. Radiologists' legal obligations now extend to the realm of digital ethics, including responsibility for the security of electronic patient data. Regulatory harmonization and strengthening of digital medical data protection policies are needed to ensure legal certainty and maintain public trust in digital healthcare services.

Keyword: Personal Data Protection, Health Law, Radiologists, Digitalization, Healthcare.

INTRODUCTION

Digital transformation in healthcare has brought about significant changes in the way medical professionals provide services (Yunus, 2025). Innovations such as electronic medical records, telemedicine, and the Picture Archiving and Communication System (PACS) in radiology have facilitated the rapid and efficient storage and access of medical information (Icanervilia et al., 2024). Patient data can now be accessed across healthcare facilities through

digital networks, facilitating diagnosis and collaboration between physicians. This system creates administrative efficiency, improves diagnostic accuracy, and accelerates the treatment process (Firdaus et al., 2025). However, this convenience also increases the potential risk of privacy breaches, as patient data becomes more vulnerable to misuse and leakage.

The development of digital technology brings both new opportunities and threats to the medical world, particularly in patient information management. The reliance of hospitals and medical personnel on electronic systems poses significant risks to data security (Asrin et al., 2024). Medical data such as X-rays, CT scans, and MRI scans constitute sensitive personal data that can have significant consequences if shared without permission (Istiqomah & Nisa, 2024). Many data breaches are caused by weak system security, a lack of digital literacy among healthcare professionals, or weak regulations governing medical data governance (Nadiroh & Wiraguna, 2025). This reality highlights the need for a stronger legal system to protect patients' rights as owners of personal data.

The need for more comprehensive regulations is increasingly apparent as information technology becomes part of daily medical care activities. Digitalization brings changes to the way patient data is stored, managed, and utilized, requiring new legal responsibilities for healthcare professionals (Yumame, 2025). Previous laws and regulations have not fully accommodated the dynamics of data protection in modern digital systems. With the enactment of Law Number 17 of 2023 concerning Health and Law Number 27 of 2022 concerning Personal Data Protection, the state is making efforts to strengthen the legal basis for medical data protection. These two laws provide a new direction for the secure and responsible management of patient data in the digital era.

These regulatory changes have major implications for the practice of radiology, which relies heavily on information technology. Radiologists work with digital data from image recording and storage to delivery to referring physicians or patients. This process requires extra care because potential breaches of confidentiality can occur at every stage (Prabowo, Muhimmah, & Kurniawan, 2017). Leaked or misused radiology data can cause moral and material harm to patients, as well as legal risks for medical personnel (Hadiyantina et al., 2023). This situation requires a strong understanding of the legal obligations and professional ethics of every radiologist involved in digital healthcare systems.

Radiologists' responsibilities extend beyond ensuring diagnostic accuracy and upholding professionalism to protecting the patient data they access and manage. Confidentiality of medical data is a universally recognized patient right (Indra, Dewi, & Wibowo, 2024). Leaks of medical information can have serious consequences, including social stigma, privacy violations, and the potential for misuse for non-medical purposes. Every professional action must be carried out with due regard for the principles of prudence, information security, and the integrity of the medical profession (Riyanto & Ratnawati, 2024). Strengthening ethical awareness and legal understanding are crucial factors to ensure that digitalization does not erode moral values or the trust between patients and doctors.

Patient data is an asset of high value both medically and legally. Any information regarding a person's health condition, examination results, and treatment records falls into the category of sensitive personal data that must be protected (Masidin, 2024). Protecting this data relates not only to technical security aspects but also to the moral responsibility of medical personnel to maintain patient privacy. Classifying medical data as sensitive personal data means that all forms of data collection, storage, and dissemination must be accompanied by the consent of the patient, the legitimate owner of the information (Tampubolon et al.,2024). Understanding data ownership rights is a crucial foundation for regulating the relationship between patients, doctors, and healthcare institutions.

The principle of patient data protection is based on several core values that must be upheld by all parties involved in healthcare. Confidentiality is the primary principle, requiring

all medical personnel not to disclose patient information without permission. Security refers to the implementation of technical and administrative measures to prevent unauthorized access to medical data (Andhani et al., 2024). Data integrity emphasizes the need to maintain the authenticity and accuracy of information to prevent manipulation. Accuracy ensures that all stored and used data is correct and up to date, while restricted access means that only authorized parties are allowed to view or use the data (Pratama et al., 2024). These five principles form the foundation of a legal protection system for patient data in the digital age.

Digital systems are bringing significant changes to the way medical data is stored and managed. The implementation of electronic medical records enables the integration of data across hospitals, clinics, and laboratories into a single platform. This technology accelerates service delivery and facilitates coordination between doctors from various disciplines (Rusman & Suwardoyo, 2022). However, the use of digital systems also increases the risk of data breaches due to cyberattacks, human error, or security weaknesses. Many data breaches in the healthcare sector stem from negligence in management or a lack of encryption in storage systems (Sidiq, 2025). This weakness requires increased digital capacity and legal awareness among healthcare professionals to ensure that electronic systems truly provide benefits without compromising patient privacy.

The digital transformation in healthcare also impacts the paradigm of the relationship between patients and providers. Patients are no longer merely recipients of medical services, but also legal entities entitled to data protection. Hospitals, clinics, and medical personnel act as data controllers and processors and must fulfill their legal obligations responsibly (Wulandari et al., 2025). Failure to safeguard patient data can result in legal consequences, both in the form of administrative sanctions and civil lawsuits. The recognition that patient data has legal status as a protected right drives the need for a more robust oversight and accountability system in all medical information management activities.

The involvement of digital technology in patient data management presents multidimensional challenges that require a balanced approach to law, ethics, and technology. The existence of strong legal instruments will be futile without the support of professional ethics and adequate technical skills from healthcare professionals. Strengthening a culture of data protection must begin with individual medical personnel's awareness of the importance of maintaining patient confidentiality and trust. Digitalization should strengthen the ethical relationship between doctors and patients, not weaken it (Sasongko et al., 2025). The application of the principle of prudence, moral responsibility, and continuous oversight will be key to success in building a safe and equitable digital health system.

The Legal Protection Theory proposed by Philipus M. Hadjon emphasizes that every individual has the right to guaranteed protection from arbitrary actions that could harm their rights (Sinaulan, 2018). In the healthcare sector, patients are legal subjects who must be protected from potential violations of their right to privacy, including the confidentiality of medical data. Legal protection is not only in the form of written regulations, but also in concrete implementation through effective oversight and law enforcement mechanisms. This concept emphasizes the state's obligation to create a system that provides every citizen with a sense of security regarding their personal data. In medical practice, legal protection includes the responsibility of healthcare professionals to ensure that patient data is not used in an unethical or unlawful manner.

The Liability Theory serves as an important foundation for assessing legal actions that cause harm to other parties (Matippanna, 2022). Medical professionals, including radiologists, have a professional responsibility for their actions, both towards patients and the data they manage. Any negligence that results in data leakage can be categorized as a legal violation that carries the consequences of sanctions. This principle of liability concerns not only individual errors but also the healthcare institutions where they work. The use of this

theory helps assess the extent to which errors and negligence can be legally accounted for in the management of digital-based patient data.

The right to privacy is a fundamental aspect underlying the concept of Data Protection Law in many countries. This right guarantees every individual control over their personal information and determines how that data is used. Internationally, regulations such as the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States have become global standards for protecting personal data, particularly medical data (Widjaja et al., 2025). Both emphasize the importance of explicit consent, transparency of data processing, and the obligation of data controllers to maintain information security. These principles serve as important references for the development of national law in Indonesia to align with global standards for patient data protection.

These theories demonstrate that patient data protection is not merely a technical matter but also reflects the values of justice, responsibility, and respect for human dignity. The law serves as a tool to maintain a balance between technological progress and individual human rights. Good regulations are insufficient without a strong awareness of professional ethics and a strong legal culture among medical personnel. Legal theory helps provide a systematic framework so that data protection policies are not merely administrative but also have a strong moral foundation. An understanding of these theories will strengthen the analytical basis for legal practices in the field of medical data protection in Indonesia.

Patient data protection ultimately embodies the right to security and respect for privacy as part of human rights. The integration of legal protection theory, legal responsibility, and the right to privacy creates a holistic approach to this issue. Balancing the public interest in improving healthcare services and the individual interest in maintaining privacy is a key challenge for policymakers. Strengthening regulations based on these legal principles will be a crucial foundation for developing a digital health system that is ethical, safe, and equitable for all parties involved.

METHOD

This research employs a normative juridical method, focusing on the study of legal norms enshrined in laws and regulations, as well as legal principles relevant to patient data protection in the digital era. The approaches employed are statutory and conceptual approaches. The statutory approach examines various legal provisions governing personal data protection and the provision of healthcare services, such as Law Number 27 of 2022 concerning Personal Data Protection, Law Number 17 of 2023 concerning Health, and Minister of Health Regulation Number 24 of 2022 concerning Medical Records. This approach aims to systematically understand the relationship between legal regulations and assess the extent to which these regulations provide effective legal protection for patients, particularly regarding electronic medical records and the responsibilities of radiologists. Meanwhile, the conceptual approach explores relevant legal doctrines and theories, such as the theory of legal protection, the theory of legal responsibility (liability theory), and the concept of the right to privacy in healthcare law. It helps interpret legal norms more deeply to explain the principles, objectives, and direction of regulatory development related to patient data protection in the era of digital healthcare. Research data were obtained from primary, secondary, and tertiary legal materials, which were then analyzed descriptively and analytically to illustrate the application of legal norms and evaluate their effectiveness on patient data protection practices and the legal responsibilities of medical personnel, particularly radiologists.

RESULTS AND DISCUSSION

Legal Basis and Changes to Patient Data Protection Regulations in the Era of Digitalization of Healthcare Services

Law Number 17 of 2023 concerning Health marks a new milestone in the implementation of the national health system, including in patient data management. This regulation introduces a more modern approach to health information systems and encourages the national implementation of electronic medical records. Articles in this law emphasize the obligation of healthcare facilities to maintain the confidentiality of patient data and regulate patients' rights to the security of their personal information. Medical records are no longer viewed simply as medical records, but as data with legal value, and must be managed with high security standards. Any misuse of data or negligence in maintaining confidentiality can result in administrative and criminal sanctions.

The provisions of the 2023 Health Law also provide the legal basis for the implementation of an integrated digital health system across agencies. The government is required to develop a national health information system that supports efficient services without neglecting the protection of personal data. The use of technologies such as cloud storage and electronic data exchange systems can only be implemented if they comply with security principles and require the consent of the data owner, the patient. This law places the responsibility on every healthcare professional to maintain the confidentiality of information obtained in the course of their professional duties. Failure to fulfill these obligations is considered a violation of medical ethics and a violation of the law, subject to sanctions in accordance with statutory provisions.

Patient data protection is also strengthened through Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This law comprehensively regulates the rights of data subjects, the obligations of data controllers, and procedures for processing and storing personal data, including health data. Patient data is considered sensitive personal data and requires the highest level of protection. All collection, use, and storage of medical data must be based on valid patient consent. The PDP Law also introduces the concept of a personal data controller, the party that determines the purpose and method of data processing, which in the healthcare sector can be a hospital or a doctor as a service provider.

The provisions in the PDP Law emphasize the principles of transparency, purpose limitation, and accountability in personal data management. Every party managing patient data is required to have a clear security policy, including a mechanism for reporting data breach incidents. Violations of these provisions can result in criminal sanctions, administrative fines, and compensation obligations. The PDP Law also establishes a personal data protection supervisory agency authorized to conduct audits, issue warnings, and impose sanctions on parties found negligent or misusing personal data. The existence of this institution strengthens the legal institutional structure in the field of data protection and increases legal certainty for patients.

Minister of Health Regulation Number 24 of 2022 concerning Medical Records serves as a technical implementation instrument for the patient data protection system in healthcare facilities. This regulation details the format, management, storage, and security of medical records, both in physical and electronic form. This regulation emphasizes that medical records are confidential legal documents and can only be accessed by authorized parties with the patient's permission. Every hospital is required to provide a secure electronic storage system, record all access to patient data, and ensure a data recovery mechanism in the event of damage or loss. This regulation also emphasizes the importance of user authentication to prevent unauthorized access to the system.

The implementation of Minister of Health Regulation No. 24 of 2022 clarifies the relationship between medical ethics principles and legal norms in medical data management.

Healthcare workers are required to maintain data confidentiality not only by virtue of their professional oath but also as a legal obligation, with consequences if violated. This regulation provides clarity regarding institutional and individual responsibilities for patient data security. Every act of data collection, storage, and distribution must be well-documented as a form of legal accountability. Thus, patient data protection is not only a moral responsibility but also a measurable and monitorable legal obligation.

Prior to the enactment of the 2023 Health Law and the 2022 Patient Data Protection Law, patient data protection in Indonesia tended to be sectoral and scattered across various regulations without a unified set of norms. Previous regulations focused more on aspects of medical ethics and professional confidentiality, as stipulated in the medical professional code of ethics. There were no legal standards explicitly regulating the protection of patient's personal data as a legal right separate from ethical obligations. This situation created a significant legal gap, especially as digital technology began to be widely implemented in healthcare facilities. When data breaches occurred, it was difficult to clearly determine legal responsibility due to the lack of specific regulations governing medical data processing.

Significant changes began to emerge following the enactment of the 2022 Personal Data Protection Law, which introduced the concept of data protection as a separate legal right. This regulation not only addresses the moral and ethical protection of patient data but also provides concrete legal sanctions for violators. Regulations regarding data controllers and processors clarify the responsibilities of each party involved in processing personal data. The 2023 Health Law further strengthens these regulations by emphasizing that patient data is part of the national health information system and must be protected from misuse. The integration of these two laws creates a more robust legal system for safeguarding patient rights in the digital age.

A comparison of the old and new regulations also reveals improvements in legal responsibility and data governance. The new regulation provides the basis for the establishment of stricter oversight mechanisms and audit requirements for data management in healthcare facilities. Each institution is required to implement a measurable data protection policy, including the appointment of a personal data protection officer to oversee compliance with the regulations. This responsibility rests not only with individual medical personnel but also with healthcare institutions as legal entities. This system strikes a balance between protecting patient rights and legal certainty for healthcare providers.

The legal obligations of medical personnel in the digital era are increasingly complex, including responsibility for protecting patient data. Physicians, including radiologists, hold a strategic position as those with direct access to sensitive patient data. Every action involving the collection, processing, and storage of data must be conducted in accordance with data protection principles as stipulated in the PDP Law and the Health Law. Failure to maintain data security can result in administrative, civil, and even criminal sanctions. This obligation reflects a paradigm shift in the medical profession, which must now understand not only clinical aspects, but also legal and information security aspects.

Hospitals and healthcare facilities, as controllers of personal data, have greater legal responsibilities. They are required to provide secure technological infrastructure, establish internal data protection policies, and ensure that all medical personnel understand their legal obligations. Any violation of data security principles can lead to legal action from both patients and data protection authorities. Hospitals cannot avoid legal liability even if data breaches occur due to technical errors or third-party negligence. The principle of vicarious liability holds healthcare institutions accountable for the actions of their healthcare personnel.

Legal implications relate not only to sanctions but also to moral obligations and the profession's reputation. Radiologists found negligent in maintaining patient data confidentiality can face disciplinary action from professional organizations in addition to

state legal sanctions. Public trust in healthcare personnel can be eroded if violations result in harm to patients. Patient data protection is not simply a formal obligation but also part of efforts to maintain public trust in the integrity of the medical profession. Legal and ethical awareness is key for healthcare personnel to adapt to regulatory demands in the era of digital healthcare.

The introduction of new regulations also creates preventive legal responsibilities. Healthcare facilities are required to conduct regular training on data security and implement effective internal monitoring systems. Regular audits and evaluations of information security systems are essential to ensure regulatory compliance. Every internal policy must be formulated in line with the legal principles established in the Patient Data Protection Law and the Health Law. This approach demonstrates that patient data protection is not merely an administrative obligation but rather part of a legal risk management system that must be implemented on an ongoing basis.

Patient data protection in the digital era requires not only strong regulations but also a commitment from healthcare providers to implement them consistently. The legal responsibilities stipulated in various regulations will not be effective without a collective awareness that data security is part of quality medical services. Any violation of data protection principles represents a systemic failure that can be detrimental to many parties. Alignment among policy, technology, and professional behavior is the foundation for the successful implementation of patient data protection in Indonesia.

Analysis and Discussion of the Implementation of Patient Data Protection and the Legal Obligations of Radiologists in the Digital Era

Regulatory changes governing patient data protection in the digital era have introduced new dynamics to Indonesia's healthcare legal system. Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) and Law No. 17 of 2023 concerning Health are two key pillars in building secure, transparent, and accountable medical data governance. The PDP Law introduces basic principles for personal data management, including the principles of legality of processing, transparency, and accountability. Meanwhile, the Health Law regulates the obligation of healthcare facility providers to protect patient data, including in the form of electronic medical records, as stipulated in Article 351. The synergy between these two laws demonstrates a paradigm shift from medical ethics-based protection to law-based protection that has clear sanctions and oversight powers.

The effectiveness of the harmonization between the PDP Law and the Health Law can be seen from the consistency of the legal principles used. Article 5 of the PDP Law affirms the data subject's right to obtain information regarding the purpose of data processing, and Article 8 affirms the right to delete personal data, while the Health Law emphasizes that all patient data is confidential and can only be accessed by authorized parties or with the patient's permission. These two regulations demonstrate the integration of sensitive data protection principles in the health sector, although challenges remain in technical alignment between implementing agencies. The role of the personal data supervisory authority, as stipulated in Article 58 of the PDP Law, is key in ensuring compliance by health service providers with the digital security principles regulated by the Ministry of Health.

The institutional aspect of patient data protection demonstrates that the personal data supervisory authority has a crucial mandate to oversee the implementation of data controller obligations. This authority is responsible for receiving reports of violations, conducting investigations, and imposing administrative sanctions. This mechanism strengthens the healthcare legal system, which previously relied solely on internal oversight by hospitals or professional associations. In its implementation, hospitals and radiology service providers are

required to have internal data protection policies, conduct regular system security audits, and appoint a personal data protection officer (DPA), as stipulated in Article 53 of the PDP Law.

The impact of the new regulations on the governance of digital radiology systems is significant. Documents resulting from examinations such as X-rays, MRIs, and CT scans are now stored electronically through the Picture Archiving and Communication System (PACS), which is connected to a network of hospitals and medical personnel. Article 297, paragraph (3) of the Health Law stipulates that electronic medical records must be stored securely by authorized parties. Digital data management requires encryption standards, user authentication, and storage policies that refer to the principle of data minimization. PACS systems that do not meet security standards can pose a risk of data leakage and have legal implications for service providers.

The legal responsibilities of radiologists are becoming increasingly complex with the increasing digitization of medical examination results. Radiologists have the authority to access, interpret, and store patient data in digital form. This obligation to maintain data confidentiality is part of their professional responsibility as stipulated in Article 296 paragraph (5) of the Health Law, which stipulates that medical personnel are required to maintain the confidentiality of patient data obtained in the course of their duties. Violations of this provision may result in administrative and even criminal sanctions if they result in data loss or misuse.

The limits of a doctor's legal liability become a critical issue when data leaks are caused by external factors, such as system errors or hacking by third parties. In this case, legal analysis must distinguish between personal and institutional liability. Article 30 of the PDP Law stipulates that data controllers are responsible for all data processing carried out within their jurisdiction, including when third parties are involved. This means that hospitals, as data controllers, have the primary legal obligation, while physicians, as data processors, are required to comply with established security policies.

The ethics of the radiology profession also require a moral commitment to protecting patients' digital data. Medical ethical standards emphasize that all medical information is confidential and should not be disseminated without the patient's consent. In the digital era, this principle has been extended to include the obligation to ensure the security of medical information systems. Cybersecurity training for radiologists has become an unavoidable necessity, given the high risk of cyberattacks on healthcare systems. Professional ethics and legal compliance complement each other in maintaining public trust in technology-based healthcare services.

The implementation of data protection regulations faces serious challenges, particularly in terms of infrastructure readiness and legal awareness of medical personnel. Many hospitals lack adequate information security systems or have not appointed personal data protection officers, as required by Article 53 of the PDP Law. This lack of preparedness poses legal risks for healthcare facilities and radiologists operating under these systems. Furthermore, weak regulatory dissemination means that most medical personnel do not understand the legal consequences of patient data protection breaches.

Inter-agency coordination is a weak point in the implementation of patient data protection. The Ministry of Health, as the health sector regulator, and the Ministry of Communication and Informatics, as the telematics authority, have roles that must be integrated with the personal data protection authority. The lack of synchronization of policies between agencies leads to overlapping oversight and law enforcement. To address this, a formal coordination mechanism is needed through government regulations or joint decrees that clearly define the division of oversight authority and responsibility.

A future normative approach should focus on regulatory integration and strengthening the capacity of healthcare sector actors. The government needs to develop national digital

security standards for the medical sector, encompassing data encryption systems, user authentication, and security incident reporting procedures. Digital law and ethics training for radiologists and other medical personnel will strengthen a culture of legal compliance in the era of healthcare digitalization. Harmonizing health regulations and personal data protection is a crucial foundation for realizing secure, ethical, and equitable patient data governance in Indonesia.

CONCLUSION

Regulatory changes through Law Number 27 of 2022 concerning Personal Data Protection and Law Number 17 of 2023 concerning Health have strengthened the legal foundation for patient data protection in Indonesia, particularly in the era of digital healthcare. Both laws emphasize that medical data is sensitive personal data that must be kept confidential in accordance with the principles of security, transparency, and accountability. The establishment of stricter norms regarding electronic medical records, access control, and sanctions for violations represents a step forward toward more responsible health data governance. However, their implementation still faces technical challenges such as weak hospital digital infrastructure, low awareness among medical personnel of cybersecurity principles, and a lack of synchronization between supervisory agencies. Radiologists are now burdened not only with the professional responsibility of establishing a diagnosis but also with the legal obligation to ensure the security of patients' digital data as part of professional ethics and compliance with national law.

The government needs to immediately develop more detailed derivative regulations to clarify the mechanisms for protecting digital medical data, particularly in the field of radiology, which relies heavily on information system-based technology. Technical standards regarding the security of test result storage, system audit obligations, and guidelines for reporting data breaches need to be comprehensively regulated to avoid overlapping authority between institutions. Strengthening legal literacy and cybersecurity awareness among medical personnel is a strategic step to foster legal awareness and digital ethics among healthcare professionals. Collaboration and harmonization between agencies such as the Ministry of Health, the Ministry of Communication and Informatics, and the Personal Data Protection Authority must be strengthened to ensure legal certainty, effective oversight, and the protection of patient rights as data subjects in the modern healthcare system.

REFERENCE

Andhani, A. Z., Ramalinda, D., Jayadi, Y., Yunengsih, Y., Pramudianto, A., Rahayu, T., . . . Muchsam, Y. (2024). *Dasar-Dasar Rekam Medis: Panduan Praktis untuk Pemula.* Yogyakarta: Penerbit KBM Indonesia.

Asrin, F., Anra, H., Irwansyah, M. A., & Pratama, E. E. (2024). Pemahaman Dampak Positif dan Negatif Perkembangan Komputer Di Bidang Kesehatan. *Jurnal Abdimas Mandiri, 8*(2), 159-168.

Firdaus, R., Syeira, K., & Wijaya, N. (2025). Transformasi Digital Sistem Informasi Kesehatan Menuju Layanan Kesehatan Yang Terkoneksi Dan Berpusat Pada Pasien. *Economics and Digital Business Review, 6*(2), 1045-1055.

Hadiyantina, S., Ayub, Z. A., Cahyandari, D., Paramitha, A. A., Ambarwati, S. D., Mustofa, Y., . . . Rahmatika, N. A. (2023). *Perlindungan Data Pribadi Dalam Bidang Rekam Medis.* Malang: Universitas Brawijaya Press.

Icanervilia, A. V., Choridah, L., Pribadi, A. W., Rahman, A., Gusti, A. M., Huwaida, A., . . . Setyawan, N. H. (2024). Evaluasi Pemanfaatan PACS dan RIS Rumah Sakit Provinsi Yogyakarta, Indonesia. *Jurnal Kesehatan Vokasional, 9*(1), 41-51.

Indra, I., Dewi, T. N., & Wibowo, D. B. (2024). Perlindungan kerahasiaan data pasien vs kewajiban membuka akses rekam medis elektronik. *Soepra Jurnal Hukum Kesehatan, 10*(1), 97-117.

Istiqomah, H., & Nisa, K. (2024). Potensi dan Tantangan Implementasi Blockchain dalam Pengelolaan Citra Medis: Sebuah Tinjauan Literatur. *Jurnal Kolaborasi Riset Sarjana, 1*(1), 56-72.

Masidin, M. (2024). URGENSI PERLINDUNGAN HUKUM DATA PRIBADI PASIEN DALAM PELAYANAN KESEHATAN BERBASIS UNDANG-UNDANG NO. 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI. *Jurnal Hukum: Officium Nobile, 1*(1).

Matippanna, A. (2022). *Hukum Kesehatan: Tanggung Jawab Hukum Rumah Sakit Terhadap Pasien Dalam Pelaksanaan Pelayanan Kesehatan.* Banyumas: AMERTA MEDIA.

Nadiroh, A., & Wiraguna, S. A. (2025). Analisis Yuridis Kebocoran Data di Layanan Kesehatan Digital: Studi Kasus Aplikasi Telemedicine di Indonesia. *Media Hukum Indonesia (MHI), 3*(2).

Prabowo, M., Muhimmah, I., & Kurniawan, R. (2017). Pemodelan Pengiriman Data Citra Medis untuk Konsultasi Radiologi. *Seminar Nasional Informatika Medis (SNIMed)*, 76-84.

Pratama, A. M., Syaiful, M., & Rahman, M. F. (2024). *Keamanan Data dan Informasi.* Bandung: Kaizen Media Publishing.

Riyanto, O. S., & Ratnawati, E. T. (2024). Hak atas informasi kesehatan dan perlindungan hukum bagi dokter: implikasi ham dalam komunikasi dokter-pasien. *Juris Humanity: Jurnal Riset Dan Kajian Hukum Hak Asasi Manusia, 3*(1), 78-88.

Rusman, A. D., & Suwardoyo, U. (2022). *Penerapan Sistem Informasi Berbasis IT Pengolahan Data Rekam Medis untuk Peningkatan Pelayanan di Rumah Sakit.* Pekalongan: Penerbit NEM.

Sasongko, H. P., Putra, R. A., Lidiyawati, H., Narko, T., & Andarmoyo, S. (2025). *Revolusi Kesehatan: Kolaborasi Teknologi, Inovasi, Dan Kebijakan.* Jambi: PT. Nawala Gama Education.

Sidiq, M. A. (2025). Perlindungan Hukum terhadap Rumah Sakit atas Kebocoran Data Rekam Medik Elektronik yang Dilakukan Oleh Peretas. *AKADEMIK: Jurnal Mahasiswa Humanis, 5*(2), 605-620.

Sinaulan, J. H. (2018). Perlindungan hukum terhadap warga masyarakat. *Ideas: Jurnal Pendidikan, Sosial, Dan Budaya, 4*(1).

Tampubolon, E. T., Putera, A. P., & Huda, M. K. (2024). Pertanggungjawaban Hukum Rumah Sakit Terkait Kebocoran Data Pribadi Pasien Berdasarkan Peraturan Perundang-Undangan. *Syntax Idea, 6*(3), 1388-1402.

Widjaja, G., Sijabat, H. H., & Dhanudibroto, H. (2025). HAK PASIEN ATAS PRIVASI DATA MEDIS: TINJAUAN LITERATUR DAN EVALUASI KEBIJAKAN. *ZAHRA: JOURNAL OF HEALTH AND MEDICAL RESEARCH, 5*(2), 12-22.

Wulandari, M., Novriyanti, T., Purwadhi, P., & Widjaja, Y. R. (2025). Implementasi Strategi Transformasi Digital dalam Meningkatkan Kualitas Pelayanan di Rumah Sakit: Studi Kualitatif. *Innovative: Journal Of Social Science Research, 5*(1), 1415-1427.

Yumame, J. (2025). DIGITALISASI PELAYANAN KESEHATAN DAN IMPLIKASINYA TERHADAP HUKUM ADMINISTRASI: STUDI LITERATUR TENTANG PEMANFAATAN TEKNOLOGI DAN PERAN REGULASI. *ADMIN: Jurnal Administrasi Negara, 3*(4), 125-133.

Yunus, M. Y. (2025). Transformasi Digital Dalam Kewirausahaan Kesehatan: Peluang Dan Tantangan Bagi Kesehatan Masyarakat. *RIGGS: Journal of Artificial Intelligence and Digital Business, 4*(3), 7639-7648.