JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v5i6

Harmonization of Regulations in Realizing Legal Certainty for the Protection of Medical Records and Personal Data

I Nyoman Widiarta[1*], I Gusti Agung Mas Rwa Jayantiari[2], Luh Nyoman Alit Aryani[3]
[1] Master Program in Health Law, Faculty of Postgraduate, Udayana University, Denpasar, Indonesia, dr.widiarta@gmail.com
[2] Master Program in Health Law, Faculty of Postgraduate, Udayana University, Denpasar, Indonesia, mas_jayantiari@unud.ac.id
[3] Master Program in Health Law, Faculty of Postgraduate, Udayana University, Denpasar, Indonesia, alit_aryani@unud.ac.id

[*]Corresponding Author: dr.widiarta@gmail.com

Abstract: This research is a normative legal study aimed at analyzing the norms governing the protection of patients' medical records under Law Number 17 of 2023 on Health and Law Number 27 of 2022 on Personal Data Protection, as a doctrinal review of related legislation. The method used is a juridical-normative approach through library research of statutory regulations, article explanations, legal doctrines, and secondary legal literature to explore the principles, rights, and obligations of data subjects and controllers. The normative analysis highlights the alignment of the principle of medical record confidentiality as stipulated in Article 177 paragraph 1 of Law Number 17 of 2023 on Health and the obligation to maintain the confidentiality of Personal Data under Article 36 of Law 27/2022, as well as patients' right to access as regulated in Article 276 of Law 17/2023. The research findings identify an overlap between the long-term retention provisions of medical records and the "right to erasure" principle, which is not specifically regulated in Law 27/2022, thereby indicating the need for harmonization of norms and technical guidelines in the health sector. These findings underscore the importance of formulating a Government Regulation to implement Article 299 of Law 17/2023 in order to bridge the obligations of data retention and the mechanisms for erasing medical data, ensuring legal certainty and the protection of patients' rights.

Keyword: Patient Medical Records, Regulatory Harmonization, Personal Data Protection

INTRODUCTION

The digitization of medical records through electronic systems in healthcare facilities has made it easier for medical personnel to access patients' medical histories quickly and centrally. This improves diagnostic accuracy and reduces medical errors caused by manual record-keeping that is prone to human error. Data integration between community health centers (puskesmas), hospitals, and financing institutions such as BPJS Health enables more coordinated and continuous patient care. Administrative processes such as appointment scheduling, insurance claims, and epidemiological reporting can be streamlined, thereby

reducing operational burdens and costs. With the introduction of the SATUSEHAT platform, health data interoperability has been strengthened, supporting evidence-based policy development across all levels of healthcare services (Ariani, 2023).

On the other hand, the advancement of digitalization also exposes serious vulnerabilities to the leakage and misuse of patients' personal data. The data breach incident involving BPJS Health in May 2021, which affected 279 million population records, raised public concern over the security of health data. An investigation by the Ministry of Communication and Information (Kominfo) found that the data samples matched the structure of BPJS records, revealing weaknesses in protection systems and access control procedures. In addition, other data breaches including passport data (34 million records), PeduliLindungi data (3.2 billion records), and MyPertamina data (45 million records) demonstrate a recurring pattern of vulnerabilities in weak electronic systems. Contributing factors include poor cybersecurity infrastructure, software vulnerabilities, phishing attacks, and even insider negligence or sabotage. These threats demand the implementation of stronger cybersecurity measures and stricter personal data protection policies within the digital health ecosystem (Herryani & Njoto, 2022).

Law Number 17 of 2023 on Health, hereinafter referred to as the Health Law, establishes the confidentiality and access rights to patient medical records as legal pillars for the protection of health data. Article 177 paragraph (1) of Law Number 17 of 2023 states that every patient has the right to the confidentiality of health information disclosed to healthcare professionals. Article 297 paragraph (3) of the Health Law obligates healthcare facilities to create, store, and maintain the confidentiality of patient medical records. Article 297 paragraph (2) regulates the procedures for patients to obtain a summary of their medical records upon request, including the application mechanism and the timeframe for provision, as well as sanctions both administrative and criminal for healthcare providers who violate the confidentiality of medical records (Kementrian Kesehatan, 2023).

Furthermore, Law Number 27 of 2022 on Personal Data Protection, hereinafter referred to as the Personal Data Protection Law, expands the scope of personal data protection to include health data as a form of "specific personal data." Article 26 of the Personal Data Protection Law grants data subjects, including patients, the rights to consent, access, correction, and deletion of their personal data. Articles 35 to 39 regulate the obligations of personal data controllers to establish technical and operational measures to protect, maintain confidentiality, and prevent unauthorized processing in accordance with the level of risk associated with the data being processed. The Personal Data Protection Law also mandates the appointment of a Data Protection Officer for large-scale data processing and stipulates both administrative and criminal sanctions for violations. Thus, the Personal Data Protection Law forms a comprehensive framework that accommodates technological advancements and modern data protection practices (Kominfo, 2022).

A comparison between Law Number 17 of 2023 and Law Number 27 of 2022 is crucial to identify overlaps, regulatory gaps, and opportunities for policy harmonization. The Health Law focuses on the confidentiality of medical secrets and the right to access medical records, while the Personal Data Protection Law governs data subjects' rights and data controllers' obligations in a broader and more detailed manner. A comparative analysis will provide insights into the benefits of applying the principles of the Personal Data Protection Law to the health sector in order to strengthen the protection of patients' medical data. These findings will serve as the basis for policy recommendations to ensure that medical record protection in the digital era is fully integrated, in line with technological advancements and international standards (Fauzi & Radika Shandy, 2022).

METHOD

Normative juridical legal research is a research method that prioritizes the use of primary legal materials by exploring legal theories, concepts, principles, and relevant legislation related to the topic under study. This research employs the statute approach, conceptual approach, and comparative approach. These approaches are carried out by examining all laws and regulations related to the legal issues being discussed. The process of collecting legal materials is conducted through library research, which includes primary, secondary, and tertiary legal materials. Once the legal materials are collected, the next step is to inventory and classify them according to the research problem formulation. These materials are then systematically organized for further analysis to answer the research questions.

RESULTS AND DISCUSSION

Regulation of Medical Records in Law Number 17 of 2023

Under Law No. 17 of 2023 on Health, the regulation of medical records is mandated to ensure service quality, protect patients' rights, and enhance the effectiveness of the health information system. Article 276 letter (e) and Article 297 paragraph (2) of the Health Law stipulate the obligation to create, store, and maintain the confidentiality of medical records, as well as the patient's right to access a summary of their medical records. Further provisions regarding the retention period of medical records are outlined in Minister of Health Regulation (Permenkes) No. 24/2022, ranging from a minimum of 2 years for non-hospital facilities to 25 years for electronic medical records. Article 283 paragraphs (4)–(5) further regulate administrative sanctions for healthcare professionals and health facilities that violate these provisions, with sanctions ranging from warnings to license revocation (Kesuma, 2023).

Article 296 of Law No. 17 of 2023 mandates that every healthcare professional providing individual health services must create a medical record for each recipient of health services. The record must be completed immediately after the service, signed with the name, date, and signature or initials of the healthcare professional, and must be stored and kept confidential by both the healthcare professional and the head of the health facility. Articles 276 and 297 of the Health Law emphasize that medical records are the property of the health facility, although recipients of health services have the right to request a summary of their records for information on the treatment they have received (Melyanti et al., 2023).

Retention provisions for hospital medical records are further regulated in Minister of Health Regulation No. 269/2008, Article 8: inpatient medical records must be retained for at least 5 years from the date of the last service, while discharge summaries and consent for medical procedures must be retained for 10 years. For non-hospital facilities, records must be kept for at least 2 years before they may be destroyed. In the digital era, Minister of Health Regulation No. 24/2022 Article 39 requires electronic medical records to be stored for at least 25 years from the patient's last visit, with destruction procedures governed by applicable laws and regulations. Furthermore, Article 32 of Permenkes No. 24/2022 obliges all parties involved to maintain the confidentiality of medical record contents, even after the patient has passed away (Irwanto et al., 2023).

Article 297 paragraph (3) of Law No. 17 of 2023 emphasizes that any healthcare professional who fails to comply with the provisions such as those in Article 283 paragraphs (4)–(5) concerning the confidentiality of health information of service recipients, along with other related provisions, may be subject to administrative sanctions. Likewise, health facilities that neglect their obligations to store and maintain the confidentiality of medical records may also face administrative penalties. According to literature, types of administrative sanctions that may be imposed include verbal warnings, written warnings, administrative fines, up to license revocation or recommendations for registration revocation, in accordance with the mechanisms stipulated in Presidential Regulation No. 90/2017 and relevant Government

Regulations. The imposition of such sanctions serves as a crucial instrument to prevent violations of medical record confidentiality, uphold professional ethics, and maintain patient trust in the healthcare system (Sri Murcittowati et al., 2023).

Regulation of Personal Data in Law Number 27 of 2022

Law Number 27 of 2022 on Personal Data Protection establishes a set of strict obligations for Personal Data Controllers, ranging from implementing operational technical measures to reporting data breach incidents, as regulated in Articles 35–46. To ensure compliance, Article 57 provides the legal basis for the imposition of administrative sanctions, ranging from written warnings to administrative fines of up to 2% of annual revenue for violations of data processing provisions. Meanwhile, criminal provisions related to the misuse of personal data are outlined in Articles 67–70, with penalties of up to six years' imprisonment and/or fines of up to IDR 6 billion. Both administrative and criminal enforcement is carried out by an independent authority established under Article 58 of the Personal Data Protection Law (Mahameru et al., 2023).

Article 35 obliges Personal Data Controllers to develop and implement operational technical measures to protect Personal Data from processing that violates statutory regulations and to determine appropriate security levels based on the nature and risk of the data. Article 36 reinforces the obligation to maintain the confidentiality of Personal Data in every processing activity, while Articles 37–39 regulate supervision of third parties, protection against unauthorized processing, and the prevention of unauthorized access through reliable electronic systems (Kusumadewi, 2023).

In the data lifecycle, Article 40 mandates that Data Controllers must cease processing within 3 × 24 hours after receiving the withdrawal of consent from the Data Subject. Article 41 regulates the postponement and restriction of processing upon the request of the Data Subject, with exceptions for national defense, public safety, or binding written agreements. Subsequently, Articles 42–43 require the termination and deletion of data when retention periods expire, processing purposes have been fulfilled, data is no longer needed, or was obtained unlawfully, followed by Article 44 which regulates the destruction of data in accordance with the retention schedule. All deletion or destruction actions must be notified to the Data Subject in accordance with Article 45 (Hakim et al., 2023).

Article 46 mandates written notification no later than 3 × 24 hours to the Data Subject and the relevant authority in the event of a data protection failure. This notification must include the type of data exposed, when and how the breach occurred, and the response and recovery efforts undertaken. Under certain conditions, the Data Controller is also required to inform the general public (Rizqiyanto et al., 2024).

Article 57 of Law Number 27 of 2022 stipulates that violations of data processing provisions, including Articles 35–46, may result in administrative sanctions in the form of written warnings, temporary suspension of processing activities, deletion or destruction of personal data, and/or administrative fines. These fines may be up to 2% of annual income or revenue, depending on the severity of the violation, to ensure proportionality of the sanctions. The imposition of administrative sanctions is carried out by an independent authority established under Article 58 of the Personal Data Protection Law, with the mandate to enforce administrative law and facilitate dispute resolution (Matheus & Gunadi, 2023).

Criminal provisions regarding the misuse of personal data are set out in Articles 67–70 of Law 27/2022. Article 67 stipulates imprisonment of up to 5 years and/or fines of up to IDR 5 billion for anyone who unlawfully and intentionally acquires, discloses, or uses another person's Personal Data without authorization. Article 68 imposes heavier penalties for those committing personal data forgery, with imprisonment of up to 6 years and/or fines of up to IDR 6 billion. Additionally, Article 69 allows for the imposition of supplementary sanctions such

as the confiscation of profits or assets obtained through the crime and compensation payments, while Article 70 expands the scope for multiple fines and additional penalties for corporations involved (Ariesta et al., 2024).

Comparative Analysis of the Health Law and the Personal Data Protection Law

Both Law No. 17 of 2023 on Health and Law No. 27 of 2022 on Personal Data Protection place confidentiality and data subject access rights as central pillars in their regulatory mechanisms. However, the Health Law is sectoral in nature, with a specific focus on medical records and detailed storage mechanisms, including retention periods and medical record presentation formats. In contrast, the Personal Data Protection Law applies broadly to all types of personal data, grounded in data protection principles such as storage limitation and processing accountability, without specifying particular retention durations (Meher et al., 2023).

Both laws require the confidentiality of personal information as an object of legal protection. Article 301 paragraph (1) of Law No. 17/2023 states that "Every healthcare professional in providing health services is required to maintain the confidentiality of the health information of the recipient of healthcare services." Similarly, Article 36 of Law No. 27/2022 obliges personal data controllers to "maintain the confidentiality of Personal Data in every processing activity." In addition, both laws grant access rights to data subjects. Article 276 letter (e) of Law No. 17/2023 stipulates that recipients of healthcare services have the right to request a summary of their medical records to understand the treatment they have received. Likewise, Law No. 27/2022 recognizes the data subject's right to "gain access and obtain a copy of Personal Data about themselves in accordance with statutory regulations" (Annan, 2024).

In terms of scope, Law No. 17/2023 is specifically limited to the health sector. Its title and provisions exclusively regulate the handling of medical information, as well as the procedures for creating, storing, and maintaining the confidentiality of medical records. It also details the format of medical records, signing requirements, and storage responsibilities within healthcare facilities, offering highly operational and technical guidance. In contrast, Law No. 27/2022 is general in nature and applies to all forms of personal data from customer data and employee information to digital service user data emphasizing data protection principles such as purpose limitation, accuracy, and storage limitation, without specifying exact retention periods in its text. It delegates the technical implementation details to Government Regulations and industry standards, making it more flexible but less specific to any single sector.

Moreover, the oversight and administrative sanction mechanisms in Law No. 17/2023 are enforced through the Ministry of Health and health professional ethics councils, whereas Law No. 27/2022 establishes an independent authority that oversees all personal data processing across sectors, with the authority to enforce administrative law and facilitate cross-industry dispute resolution (Manurung & Thalib, 2022).

Implementation Challenges

In general, the implementation of electronic medical records (EMRs) and personal data protection regulations faces two major challenges: first, a conflict between the "right to erasure" stipulated in Law No. 27/2022 and the immutable long-term retention obligations of electronic medical records; and second, the limited capacity of healthcare facilities and difficulties in enforcing sanctions on the ground. This fundamental conflict raises concerns about dual compliance obligations that may create legal loopholes, while inadequate infrastructure, human resources, and supervisory mechanisms threaten the effectiveness of regulations and the protection of patients' rights (Herisasono, 2024).

The Personal Data Protection Law (Law No. 27/2022) states that patient health data may only be stored "as long as necessary" and must be deleted or anonymized after the retention period ends. On the other hand, Article 39 of Minister of Health Regulation No. 24/2022 obliges healthcare facilities to retain electronic medical records for at least 25 years from the patient's last visit. This creates a normative overlap between long-term retention obligations and the data subject's right to erasure, thus requiring harmonization through implementing regulations that clarify priorities and technical mechanisms (Disemadi et al., 2023).

Furthermore, the Indonesian Hospital Association (PERSI) highlights the risk of fraud if medical records can be completely erased for example, the deletion of HIV records to avoid insurance claim rejection. On the other hand, the absence of clear technical guidelines in the Personal Data Protection Law and Ministerial Regulations regarding the exemption of certain types of medical records from the erasure mechanism adds uncertainty to implementation at healthcare facilities. Therefore, firm implementing regulations are needed to define which data types can be deleted and to establish procedures for migration or transfer of medical data while maintaining the integrity of medical records (Sinaga, 2020).

Research conducted in various healthcare facilities shows that the lack of support from healthcare workers and IT infrastructure is a major barrier to EMR adoption. A J-Innovative study identified inadequate IT systems, lack of healthcare worker support, and data security challenges as key obstacles. Additionally, Ghazisaeidi et al. (2021) in JMIKI emphasized the limited readiness of medical personnel, medical record officers, and patients in using electronic systems (Ulfah & Nugroho, 2020).

At the primary care level (Puskesmas), infrastructure limitations such as unstable internet connections, inadequate hardware, and a shortage of skilled IT personnel result in long registration queues and frequent server disruptions, undermining the reliability of Hospital Management Information Systems (SIMRS). PERSI data from 2022 shows that of the 3,000 hospitals in Indonesia, only around 50% have adopted EMRs, and only 16% are operating them optimally, reflecting limited capacity in managing and maintaining the systems.

The monitoring mechanism set out in Article 41 of Minister of Health Regulation No. 24/2022 grants supervisory authority to the Minister, governors, and regents/mayors. However, in practice, there is a shortage of trained inspectors and budget for routine audits. Moreover, the high costs of EMR implementation and operations including infrastructure investment, software licensing, and staff training often exceed the budget allocations of healthcare facilities, making delays in upgrades or maintenance common. This combination of resource limitations and weak oversight demands improved inter-agency coordination, enhanced technical capacity, and sustainable funding to ensure regulatory compliance and protect patients' rights (Sukmadilaga & Rosadi, 2020).

CONCLUSION

Law No. 17 of 2023 on Health mandates the confidentiality of medical records under Article 297 paragraph (3), while Law No. 27 of 2022 on Personal Data Protection affirms data confidentiality in Article 36. However, the two laws have not yet been harmonized, resulting in multiple interpretations in practice. Furthermore, studies on the implementation of the Personal Data Protection Law reveal the absence of specific technical guidelines for medical data, including standards for encryption, interoperability, and exceptions to the "right to erasure" for medical records, making it difficult for healthcare facilities to design appropriate Standard Operating Procedures (SOPs). Lastly, the low level of understanding and readiness of healthcare facility personnel regarding personal data protection as revealed in studies on the implementation of patients' rights and obligations emphasizes the need for ongoing training and public outreach programs to ensure regulatory compliance at all levels of healthcare services. To address these issues, first, a Government Regulation or Minister of Health

Regulation should be issued to explicitly harmonize Article 297 paragraph (3) of Law No. 17/2023 with Articles 36–44 of Law No. 27/2022, establishing priorities for data retention and mechanisms for medical data erasure to avoid conflict. Second, the Ministry of Communication and Information (Kominfo) and the Ministry of Health should develop specific technical guidelines for personal data protection in the health sector, covering encryption standards, interoperability formats, Privacy Impact Assessment templates, and exceptions to the right to erasure for critical clinical data. Third, the implementation of technical training and certification in data protection for healthcare workers, IT staff, and medical records officers supported by e-learning modules and real case studies of data breaches should be prioritized to foster a culture of compliance and risk awareness across all healthcare facilities.

REFERENCE

Annan, A. (2024). Tinjauan Yuridis Perlindungan Data Pribadi Pada Sektor Kesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022. *SYNERGY: Jurnal Ilmiah Multidisiplin*, *1*(4), 247–254.

Ariani, S. (2023). Analisis Keberhasilan Implementasi Rekam Medis Elektronik Dalam Meningkatkan Efisiensi Dan Mutu Pelayanan. *Jurnal Kesehatan Dan Kedokteran*, *2*(2), 7–14. https://doi.org/10.56127/jukeke.v2i2.720

Ariesta, K., Anggara, D., Minggu, I. M., Wayan, W. I., & Jaya, K. (2024). *Analisis Hukum Terhadap Pencurian Data Administrasi Kependudukan Dalam Perspektif Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Pendahuluan*. *6*(3), 330–335.

Disemadi, H. S., Sudirman, L., Girsang, J., & Aninda, M. (2023). Perlindungan Data Pribadi di Era Digital: Mengapa Kita Perlu Peduli? *Sang Sewagati Journal*, *1*(2), 67–90. https://journal.uib.ac.id/index.php/sasenal/article/view/8579

Fauzi, E., & Radika Shandy, N. A. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Jurnal Lex Renaissance*, *7*(3), 445–461. https://doi.org/10.20885/jlr.vol7.iss3.art1

Hakim, G., Kaimuddin Haris, O., & Mohammad, M. (2023). Analisis Perbandingan Hukum Mengenai Regulasi Perlindungan Data Pribadi Antara Uni Eropa dan Indonesia Comparative Analysis of Laws Concerning Personal Data Protection Regulations Between the European Union and Indonesia. *Halu Oleo Legal Research* |, *5*(2), 443–453. https://ojs.uajy.ac.id/index.php/jik/article/view/682.

Herisasono, A. (2024). *Perlindungan Hukum terhadap Privasi Data Pasien dalam Sistem Rekam Medis Elektronik Legal Protection of Patient Data Privacy in Electronic Medical Record Systems*. *7*(12), 4677–4681. https://doi.org/10.56338/jks.v7i12.6620

Herryani, M., & Njoto, H. (2022). Perlindungan Hukum Terhadap Kebocoran Data Pribadi Konsumen Online Marketplace. *Transparansi Hukum*, *5*(1), 110. http://ojs.unik-kediri.ac.id/index.php/transparansihukum/article/view/2274

Irwanto, E. L., Syofyan, S., Mannas, Y. A., Hukum, F., Andalas, U., Hukum, F., Andalas, U., Hukum, F., & Andalas, U. (2023). Urgensi pembuktian rekam medis elektronik dalam perspektif hukum di indonesia. *Jurnal UNES Law Riview*, *5*(4), 1641–1653.

Kementrian Kesehatan. (2023). *Undang-undang Nomor 17 Tahun 2023 tentang Kesehatan*.

Kesuma, S. I. (2023). Rekam Medis Elektronik Pada Pelayanan Rumah Sakit Di Indonesia: Aspek Hukum Dan Implementasi. *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora*, *1*(1), 195–205.

Kominfo. (2022). UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI. *Kominfo*, *016999*, 457–483.

Kusumadewi, D. L. (2023). Urgensi Perlindungan Data Pribadi Pada Sistem Elektronik Untuk Anak Di Bawah Umur Di Indonesia Serta Perbandingan Regulasi Dengan Uni Eropa

(General Data Protection Regulation). *Lex Patrimonium*, *2*(2). https://scholarhub.ui.ac.id/lexpatri Part

Mahameru, D. E., Nurhalizah, A., Wildan, A., Haikal, M., & Rahmadia, M. H. (2023). *Implementasi Uu Perlindungan Data*. *5*(20), 115–131.

Manurung, E. A. P., & Thalib, E. F. (2022). Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan Uu Nomor 27 Tahun 2022. *Jurnal Hukum Saraswati (JHS)*, *4*(2), 139–148.

Matheus, J., & Gunadi, A. (2023). Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU. *Justisi*, *10*(1), 20–35. https://doi.org/10.33506/jurnaljustisi.v10i1.2757

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

Melyanti, H., Lindawaty Suherman Sewu, P., & Author, C. (2023). Perlindungan Data Pribadi Dalam Pengaturan Rekam Medis Elektronik Berdasarkan Perundang-Undangan Indonesia Dihubungkan Dengan Asas-Asas Hukum. *JIM: Jurnal Ilmiah Mahasiswa Pendidikan Sejarah*, *8*(3), 1415–1422.

Rizqiyanto, N., Rohman, A., & Raya, F. (2024). Politik Hukum Pembentukan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Media Hukum Indonesia (MHI)*, *2*(2), 1–14.

Sinaga, E. M. C. (2020). Formulasi Legislasi Perlindungan Data Pribadi. *Jurnal RechtVinding*, *9*(2), 237–256.

Sri Murcittowati, P. A., Wirajaya, M. K. M., Astuti, I. W., Kartika, I. G. A., & Farmani, P. I. (2023). Pengaturan Pengaktifan Kembali Rekam Medis Elektronik pada Rumah Sakit X Kota Denpasar. *Jurnal Kesehatan Vokasional*, *8*(4), 244. https://doi.org/10.22146/jkesvo.89228

Sukmadilaga, A., & Rosadi, S. D. (2020). UPAYA HUKUM TERHADAP PELANGGARAN IMPLEMENTASI INTERNET OF THINGS (IoT) DIBIDANG PELAYANAN KESEHATAN MENURUT KETENTUAN PERLINDUNGAN DATA PRIBADI. *Jurnal Suara Keadilan*, *21*(2), 205–221. https://doi.org/10.24176/sk.v21i2.5694

Ulfah, I. F., & Nugroho, A. B. (2020). Menilik Tantangan Pembangunan Kesehatan di Indonesia: Faktor Penyebab Stunting di Kabupaten Jember. *Jurnal Sosial Politik*, *6*(2), 201–213. https://doi.org/10.22219/sospol.v6i2.12899