ORIGINAL ARTICLE

Jurnal Dharmaputra Hukum Kesehatan (*JDHK*) 2025, Volume 1, Number 2: 47-52

The legal status of electronic medical records and health data privacy in Indonesia: Current regulations, gaps, and future directions

Garry Stefiano Wulyardhi[1], Gede Krisna Udiana[2*]

[1]Family Communication Forum of Retired Red Beret
[2]Legal Unit, Wangaya Regional Hospital, Denpasar

*Corresponding author:
Gede Krisna Udiana; Legal Unit, Wangaya Regional Hospital, Denpasar;
udiana.krisna@gmail.com

Received: 2025-09-02
Accepted: 2025-12-01
Published: 2025-12-31

ABSTRACT

Introduction: Indonesia's healthcare system is undergoing digital transformation through mandatory Electronic Medical Records (EMR) under Regulation No. 24 of 2022 and the Health Omnibus Law (Law No. 17 of 2023). While EMR enhances data integration via SATUSEHAT, it raises privacy concerns under the Personal Data Protection Law. This study aims to assess the adequacy of Indonesia's legal framework governing EMR and health data protection.

Methods: This study applies a normative-juridical method complemented by empirical analysis. It reviews relevant statutes, implementing regulations, and academic literature on EMR and data protection, alongside secondary empirical data from institutional reports and documented cybersecurity incidents. The analysis focuses on regulatory harmonization, consent mechanisms, government access to health data, and data subject rights.

Results: The findings indicate that EMR implementation in Indonesia is supported by a legitimate normative foundation but remains operationally fragile. Regulatory inconsistencies persist between health sector regulations and the personal data protection regime, particularly concerning state access to medical data, informed consent, and the right to erasure. Empirically, implementation is constrained by cybersecurity vulnerabilities, unequal digital infrastructure readiness in community health centers, and limited human resource capacity, increasing legal and liability risks.

Conclusion: While Indonesia's EMR policy reflects progress toward digital health governance, enforcement of privacy protection remains underdeveloped. Strengthening the system requires clearer implementing regulations, improved cybersecurity standards, and robust institutional oversight to ensure a rights-based and sustainable digital health ecosystem.

Keywords: Electronic medical record (EMR), health data privacy, Indonesia, legal framework, regulatory gaps.
Cite This Article: Wulyardhi, G.S, Udiana, G.K. 2025. The legal status of electronic medical records and health data privacy in Indonesia: Current regulations, gaps, and future directions. *Jurnal Dharmaputra Hukum Kesehatan* 1(2): 47-52

INTRODUCTION

The trajectory of healthcare governance in Indonesia is currently characterized by a paradigm shift from fragmented, paper-based health administration toward an integrated, digital health ecosystem. This transition constitutes not merely a technological advancement, but a structural reconfiguration of the legal, institutional, and operational frameworks that regulate the management, use, and protection of health information. Historically, medical records in Indonesia were governed by the Minister of Health Regulation No. 269 of 2008, a regulation conceptualized in an era where digital records were supplementary to physical files. However, the exigencies of modern healthcare, highlighted by the COVID-19 pandemic and the need for real-time epidemiological data, accelerated the obsolescence of this manual regime. In response, the Ministry of Health enacted Permenkes No. 24 of 2022 on Medical Records, which explicitly mandates that every healthcare facility, ranging from tertiary referral hospitals to independent medical practices, must transition to Electronic Medical Records (EMR).[1] This regulation set a definitive compliance deadline of the end of 2023, effectively outlawing the exclusive use of paper records for clinical documentation in the long term.[2] This mandate serves as the regulatory cornerstone for the Ministry's broader "Health Technology Transformation," the sixth pillar of the national health transformation agenda.[1]

Alongside this transformation, Indonesia's legal framework experienced a major development with the enactment of Law No. 27 of 2022 on Personal Data Protection (UU PDP). This law introduced, for the first time, a comprehensive and cross-sectoral data protection regime, formally recognizing health data and medical information as a category of specific personal data.[3] As a result, healthcare providers are now subject to the highest standards of data security and legal responsibility, significantly increasing their exposure to legal risk. The regulatory landscape was further reshaped by the enactment of Law No. 17 of 2023 on Health, which consolidated and replaced eleven prior statutes, including the Medical Practice Law of 2004 and the former Health Law of 2009.[4] While reaffirming the state's authority over national health information systems, the Omnibus Health Law also seeks to align this authority with patient rights and the enhanced data protection standards established under the Personal Data Protection Law.[5]

Despite extensive legislative efforts, the integration of these regulatory frameworks has produced legal uncertainty and potential normative conflicts. One key issue arises from the requirement for healthcare facilities to centralize health data through the SATUSEHAT platform, which reflects the state's role in managing national health information systems, while at the same time individuals are granted strong privacy protections under the Personal Data Protection Law.[6] In addition, the concept of public interest as a legal basis for processing health data without consent is defined broadly in health sector regulations, creating potential tension with the stricter principles of necessity and proportionality reflected in the Personal Data Protection Law and international privacy standards.

Furthermore, the gap between de jure mandates and de facto implementation remains pronounced. Empirical studies and audit reports from 2024 demonstrate that many healthcare facilities, particularly in rural areas, continue to face significant constraints related to human resources, financing, methods, and technological capacity. Infrastructure limitations, including unstable internet connectivity and outdated hardware, undermine compliance with legal requirements on data availability and integrity.[2] At the same time, the cybersecurity environment has grown increasingly hostile, as reflected in reports by the National Cyber and Crypto Agency (BSSN) documenting millions of traffic anomalies and targeted ransomware attacks against critical infrastructure.[7] These conditions expose unresolved questions of legal liability and accountability for healthcare providers in the event of data breaches, thereby underscoring the need for systematic legal scrutiny. Accordingly, this study aims to assess the adequacy of Indonesia's legal framework governing electronic medical records by examining their legal validity and evidentiary status, evaluating regulatory harmonization across health and data protection laws, analyzing implementation challenges related to cybersecurity, infrastructure, and human resources, and formulating legal and policy recommendations to strengthen health data protection.

METHODS

Search Strategy and Material Selection

Literature searching was conducted across major academic databases and relevant scholarly platforms, focusing on publications from the past five years to capture recent developments in electronic medical records and health data protection in Indonesia. Search terms included combinations of "electronic medical records," "health data privacy," "personal data protection law," "legal framework," "SATUSEHAT," "digital health governance," "cybersecurity," and "Indonesia." Relevant statutes, government and ministerial regulations, agency guidelines, court decisions, and policy documents were reviewed as primary legal materials, alongside secondary sources such as peer-reviewed journals, institutional cybersecurity reports, policy roadmaps, and legal updates, to ensure comprehensive coverage of both legal norms and implementation practices.

Inclusion and Exclusion Criteria

Included sources comprised peer-reviewed articles, authoritative legal documents, policy analyses, and empirical studies examining the regulatory and operational dimensions of electronic medical records in Indonesia, with particular attention to the SATUSEHAT platform and the implications of the Personal Data Protection Law for healthcare. Empirical studies applying analytical frameworks to assess EMR readiness were prioritized to provide implementation context. Excluded materials included studies published before 2020 unless relevant for historical comparison, general cybersecurity literature lacking a health sector focus, and opinion-based articles without statutory or regulatory analysis.

Data Extraction and Synthesis

Each selected source was assessed using adapted legal and policy appraisal criteria focusing on normative clarity, regulatory coherence, implementation feasibility, and identified legal or operational gaps in electronic medical record governance. Extracted data were organized into thematic clusters covering the legal status and evidentiary value of EMR, data protection and cybersecurity governance, and implementation practices at the healthcare facility level. A thematic synthesis approach was applied to integrate normative legal analysis with empirical evidence from institutional reports and implementation studies. Legal provisions were systematically compared with documented implementation practices to identify regulatory inconsistencies, enforcement weaknesses, and structural factors contributing to gaps between legal obligations and operational realities.

RESULT AND DISCUSSION

The Legal Status and Architecture of Electronic Medical Records

The transition to Electronic Medical Records in Indonesia constitutes a fundamental redefinition of the legal status of medical records rather than a mere change in documentation format. This transformation is primarily governed by Minister of Health Regulation No. 24 of 2022, which operates as a lex specialis within the broader framework of the Electronic Information and Transactions Law and national health legislation. Permenkes No. 24 of 2022 defines Electronic Medical Records as medical records created and managed through an electronic system for the administration of medical documentation and establishes a mandatory obligation for all healthcare facilities to implement EMR systems. The regulation eliminates discretionary use of paper-based records, allowing manual documentation only as a temporary contingency during system failures.[1] This mandatory regime is further reinforced by Law No. 17 of 2023 on Health, which integrates EMR into the National Health Information System and links compliance to healthcare facility accreditation and operational licensing.[4]

From an evidentiary perspective, EMRs play a central role in civil, criminal, and professional accountability proceedings. Article 5 of the Electronic Information and Transactions Law explicitly recognizes electronic information and documents as valid legal evidence, thereby extending the scope of documentary proof under procedural law.[8] However, the admissibility of EMRs is contingent upon compliance with strict integrity requirements. Permenkes No. 24 of 2022

mandates that EMR systems ensure data integrity through comprehensive audit trails, including the preservation of original entries, layered corrections, timestamps, and user identification.[1] Systems that permit unrecorded deletions or alterations fail to meet legal validity standards and expose healthcare providers to potential liability for evidence manipulation or spoliation in malpractice disputes.[8]

Recent regulations also clarify the legal distinction between ownership of the medical record document and ownership of the information it contains. Under Article 25 of Permenkes No. 24 of 2022, the medical record document is owned by the healthcare facility, which bears responsibility for its management, storage, and security. Conversely, Article 26 affirms that the substantive content of the medical record belongs to the patient, consistent with the Personal Data Protection Law's recognition of individuals as data subjects. This dichotomy establishes a fiduciary relationship in which healthcare providers act as custodians of patient data. While patients retain rights to access, confidentiality, and data summaries, healthcare facilities are bound by statutory retention obligations, including a minimum retention period of 25 years for electronic medical records, which limits the patient's ability to demand deletion of source records.[1]

Health Data Privacy Governance in Indonesia

The regulatory regime governing health data privacy in Indonesia has become increasingly complex due to the interaction between sector-specific health regulations and the general personal data protection framework. Law No. 27 of 2022 on Personal Data Protection fundamentally reclassifies health data and medical information as specific personal data, thereby placing them within the highest tier of legal protection. This classification carries significant legal implications, as the processing of specific personal data is generally subject to explicit consent requirements, enhanced security standards, and the obligation to conduct Data Protection Impact Assessments for high-risk processing activities. As a consequence, healthcare providers are required to implement advanced technical and organizational safeguards, including data encryption, strict access controls, and robust identity management systems, exceeding the standards applicable to general personal data.[3]

Notwithstanding these protections, a normative conflict arises in relation to the legal basis for health data processing within the national digital health ecosystem. Minister of Health Regulation No. 24 of 2022 and the Health Omnibus Law mandate that all healthcare facilities integrate electronic medical records with the Ministry of Health through the SATUSEHAT platform to support a unified national health information system.[1] While the Personal Data Protection Law generally requires consent for the processing of specific personal data, it provides exceptions for processing based on public interest and vital interests. In practice, the Ministry of Health relies on the public interest exception to justify mandatory data integration without requiring individualized patient consent.[6] However, the scope of public interest in this context remains insufficiently defined in derivative regulations, creating legal uncertainty and raising concerns regarding potential overreach. Legal scholarship highlights the risk that an expansive interpretation of public interest may undermine the data minimization principle enshrined in the Personal Data Protection Law, particularly in the absence of a government regulation specifying the limits of ministerial access to granular clinical data versus aggregated public health information.[9] Current implementation trends suggest broad access to detailed clinical records, a practice that may invite constitutional scrutiny under the right to privacy.[6]

Further tension emerges between data subject rights and statutory data retention obligations. The Personal Data Protection Law grants individuals the right to erasure, allowing data subjects to request the deletion of personal data under certain conditions. However, this right conflicts with health sector regulations requiring electronic medical records to be retained for a minimum period of 25 years, reflecting their function as legal safeguards in medical malpractice proceedings. Legal interpretation generally supports the view that statutory retention obligations constitute a lawful basis that overrides the right to erasure during the mandatory retention period. Nevertheless, once this period expires, personal health data should be destroyed or anonymized. The absence of clear and standardized protocols for post-retention data management across healthcare facilities represents a latent compliance risk and highlights a critical gap in the current regulatory framework.[10]

Implementation Challenges: The Gap Between Law and Reality

Despite an ambitious regulatory framework, the implementation of Electronic Medical Records in Indonesia reveals substantial systemic challenges that undermine legal compliance. Empirical studies employing Fishbone and PIECES analytical frameworks consistently identify four interrelated barriers, namely human resources, technological infrastructure, operational methods, and financial capacity. Among these, infrastructure deficits pose a direct threat to the legal principle of data availability. In remote and underserved regions, many community health centers experience unstable internet connectivity and unreliable electricity supply, which disrupt access to cloud-based EMR systems and integrated platforms such as BPJS PCare. As a result, healthcare workers are often compelled to revert to manual documentation or delay services, practices that conflict with the mandatory EMR regime.[2] These challenges are compounded by outdated hardware incapable of supporting contemporary encryption standards, as well as the continued use of unlicensed operating systems in resource-limited facilities, both of which compromise data integrity and system security.[11]

Human resource constraints further exacerbate implementation failures. Multiple studies identify limited digital literacy among segments of the health workforce, particularly older staff, as a critical barrier to effective EMR use.[2] This deficiency increases the risk of data entry errors and insecure practices, such as password sharing or improper credential storage, which directly violate statutory data protection obligations.[11]

Moreover, although Permenkes No. 24 of 2022 implicitly requires the availability of dedicated information technology support and medical record professionals, many primary healthcare facilities lack the financial capacity to recruit specialized personnel. Consequently, clinical staff are frequently required to assume technical roles beyond their competencies, increasing operational errors and detracting from patient care.[12]

These structural weaknesses are further magnified by significant cybersecurity vulnerabilities within the healthcare sector. The BSSN reported more than 330 million traffic anomalies in 2024, with healthcare institutions emerging as high-value targets for ransomware and data exfiltration attacks.[7] Common technical deficiencies include unpatched software, weak authentication mechanisms, and the absence of network segmentation. High-profile incidents, such as the breach of the e-HAC system affecting over one million users and reported leaks involving national health insurance data, demonstrate that even centralized state-managed systems remain highly vulnerable.[13] Collectively, these findings suggest that compliance with the security obligations mandated by the Personal Data Protection Law remains largely aspirational, exposing healthcare providers and state institutions to substantial legal and reputational risk.

Table 1. Implementation Gaps and Legal Implications

Domain	Operational Reality (The Das Sein)	Legal Mandate (The Das Sollen)	Legal Consequence of Gap
Connectivity	Frequent internet downtime in rural health facilities	Health data must be continuously available 24 hours a day as required by Minister of Health Regulation No. 24 of 2022	Violation of service standards and potential negligence claims when healthcare delivery is delayed
Security	Use of shared passwords lack of encryption and outdated operating systems	Health data classified as specific personal data must receive enhanced protection under the Personal Data Protection Law	Risk of administrative fines up to two percent of annual revenue and potential criminal liability in cases of negligence
Interoperability	Recurrent failures in data bridging between hospital information systems and BPJS or SATUSEHAT platforms	Full system integration is mandatory under the Omnibus Health Law	Inaccurate or incomplete medical records resulting in integrity violations and possible administrative sanctions including loss of accreditation
Consent	Data sharing based on implied consent without granular patient control options	Explicit consent is required for specific data processing activities under the Personal Data Protection Law	Violation of data subject rights and invalid legal basis for data processing

Liability and Enforcement in Electronic Medical Record Governance

The interaction between the Health Law, the Electronic Information and Transactions Law, and the Personal Data Protection Law establishes a multi-layered liability and enforcement regime for healthcare providers, making legal compliance a central component of institutional risk management. At the administrative level, healthcare facilities face immediate regulatory exposure for non-compliance with EMR and data protection obligations. Sanctions under Minister of Health Regulation No. 24 of 2022 and Article 57 of the Personal Data Protection Law range from written warnings and temporary suspension of data processing to data deletion orders and administrative fines. Of particular significance is the introduction of administrative fines of up to two percent of annual revenue under the Personal Data Protection Law, which represents a substantial financial risk for large hospital groups and elevates data protection compliance to a strategic governance issue. In addition, failure to comply with mandatory EMR implementation directly threatens facility accreditation, potentially disrupting cooperation with the national health insurance system and undermining the financial viability of healthcare providers.[1]

Beyond administrative sanctions, civil liability provides patients with a direct avenue for legal redress. Under Article 1365 of the Civil Code, data breaches resulting from negligent conduct, such as failure to update software or adequately train personnel, may constitute unlawful acts giving rise to claims for both material losses and immaterial harm, including psychological distress. These civil remedies are reinforced by Article 12 of the Personal Data Protection Law, which explicitly grants data subjects the right to seek compensation for violations of data protection obligations. In such cases, the burden of proof may shift to the data controller, requiring healthcare providers to demonstrate that adequate preventive measures were in place and that no negligence occurred.[13]

Criminal liability applies in cases of severe or intentional misconduct. The Personal Data Protection Law criminalizes the unlawful collection or disclosure of personal data, with penalties including imprisonment of up to five years and fines reaching IDR 5 billion.[14] Additionally, the Electronic Information and Transactions Law imposes severe sanctions for the manipulation or falsification of electronic medical records, including penalties of up to twelve years' imprisonment where records are altered to conceal malpractice.[15] Importantly, the Personal Data Protection Law recognizes corporate criminal liability, allowing hospitals or healthcare corporations to be held directly accountable where offenses are committed for institutional benefit, with sanctions

extending beyond fines to include asset seizure or operational closure.[13]

Future Directions of Electronic Medical Records Governance in Indonesia

The future of Indonesia's digital health ecosystem is structurally anchored in the SATUSEHAT platform and the Ministry of Health's strategic roadmap for 2025–2029, positioning electronic medical records as the backbone of an integrated national health information system. SATUSEHAT is designed as a "system of systems" that connects thousands of heterogeneous EMR platforms, including hospital information systems and primary care applications, into a unified digital network. This architecture enables longitudinal portability of medical records, allowing clinical information to follow patients across regions and facilities, thereby reducing redundant diagnostic procedures and mitigating medication errors when patients seek care in different provinces.[16] In the 2024–2025 phase, policy priorities have shifted toward expanding integration beyond hospitals to include pharmacies, laboratories, and private clinics, alongside an ambitious plan to consolidate more than 400 fragmented health applications into the SATUSEHAT ecosystem to reduce administrative complexity and improve interoperability.[17]

The 2025–2029 SATUSEHAT roadmap further signals a strategic pivot toward strengthening health human resources and governance structures. A central objective of this phase is the digitization of health workforce management, encompassing competency tracking, professional licensing, and workforce distribution to enable evidence-based planning and policy formulation. Equally important is the roadmap's explicit emphasis on improving data governance, reflecting institutional recognition of existing weaknesses in data standardization, quality assurance, and security enforcement. Planned interventions include the development of standardized data dictionaries, stricter data validation mechanisms, and tighter enforcement of cybersecurity protocols across connected systems.[18]

In parallel, the role of the BSSN is expected to expand significantly in shaping compliance norms. Through Regulation No. 8 of 2024, BSSN has standardized security audit requirements for electronic government systems, and although private hospitals are not formally categorized as SPBE entities, their technical dependence on SATUSEHAT effectively subjects them to comparable security expectations. This regulatory trajectory suggests that compliance with BSSN-standard cybersecurity audits may soon become a de facto prerequisite for maintaining connectivity to the national health data platform.[19]

Taken together, these findings highlight the evolution of electronic medical records in Indonesia into a legally binding instrument with clinical, regulatory, and evidentiary significance, supported by a solid normative framework under Minister of Health Regulation No. 24 of 2022, the Personal Data Protection Law, and the Health Law. However, substantial gaps persist between legal mandates and practical implementation, driven by limitations in human resources, infrastructure, governance capacity, and cybersecurity readiness, which continue to threaten data availability and confidentiality and amplify systemic risks within the centralized SATUSEHAT architecture, as reflected in rising anomaly reports by BSSN. At the same time, unresolved tensions between public health surveillance objectives and individual privacy rights, particularly due to the absence of clear implementing rules on the proportionality of public interest access, pose ongoing legal and ethical challenges. This study is limited by its reliance on normative legal analysis and secondary data, which may not fully capture regional implementation dynamics or rapid regulatory changes. Future research incorporating field-based empirical assessments and comparative international perspectives would be valuable in validating and extending the findings of this study.

CONCLUSION

In conclusion, the legal status of electronic medical records in Indonesia has been firmly established through recent regulatory developments, reflecting significant progress in integrating digital health governance with national data protection standards. However, substantial gaps persist between existing regulations and their practical enforcement, particularly in safeguarding health data privacy amid centralized data management and growing cybersecurity threats. Ambiguities in regulatory harmonization, limitations in institutional capacity, and the absence of detailed implementing instruments continue to weaken accountability and legal certainty. Addressing these shortcomings requires clearer derivative regulations, strengthened cybersecurity governance, and enhanced institutional oversight to guide future implementation. These measures are essential to ensure that Indonesia's evolving digital health system is legally coherent, protective of individual privacy rights, and sustainable in the long term.

AUTHOR CONTRIBUTIONS

GSW developed the study concept, designed the methodology, and prepared the initial manuscript draft. GKU served as the corresponding author, conducted data extraction, provided supervision, and contributed to manuscript review and revision. Both authors jointly reviewed and approved the final version of the manuscript for publication.

FUNDING

This study received no external funding.

CONFLICT OF INTEREST

The authors declare no conflicts of interest relevant to this study.

ETHICAL CONSIDERATIONS

Ethical approval was not required for this study.

REFERENCES

1. Kementerian Kesehatan Republik Indonesia. Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis. Jakarta: Kementerian Kesehatan Republik Indonesia; 2022.
2. Risnawati, Purwaningsih E. Analisis Hambatan Dalam Implementasi Rekam Medis Elektronik di Puskesmas Karang Asam Samarinda. J Pengabdi Kpd Masy Nusant. 2024;5(2):1603–8.
3. Pemerintah Republik Indonesia. Undang-Undang Republik Indonesia Nomor 27 Tahun

2022 tentang Perlindungan Data Pribadi. Jakarta: Pemerintah Republik Indonesia; 2022.
4. Pemerintah Republik Indonesia. Undang-Undang Republik Indonesia Nomor 17 Tahun 2023 tentang Kesehatan. Jakarta: Pemerintah Republik Indonesia; 2023.
5. Muhafid, Wildan, Pratama PA, Fikri AM. Transformasi UU No . 17 Tahun 2023 dalam Mendorong Sistem Kesehatan yang Insklusif dan Berkelanjutan (Tinjauan Yuridis Normatif dalam Analisis Peluang dan Tantangan). JIHHP J Ilmu Hukum, Hum dan Polit. 2025;5(6):5352–67. Available from: 10.38035/jihhp.v5i6
6. Seputra HR, Kuntardjo C, Riyandini KM, Purwanto NZ. Protection of Personal Data in Electronic Medical Records (RME) in Healthcare Facilities Reviewed from a Human Rights Perspective. RECHTSVINDING. 2025;3(1):35–42. Available from: 10.59525/rechtsvinding.v3i1.665
7. Badan Siber dan Sandi Negara (BSSN) RI. Lanskap Keamanan Siber Indonesia 2024. Jakarta: Badan Siber dan Sandi Negara (BSSN) Republik Indonesia; 2024.
8. Juwita N. Analisis Hukum Penggunaan Rekam Medis Elektronik di Rumah Sakit. Rio Law J. 2025;1(2). Available from: 10.36355/rlj.v6i1
9. Indra, Dewi TN, Wibowo DB. Perlindungan Kerahasiaan Data Pasien vs Kewajiban Membuka Akses Rekam Medis Elektronik. Soepra J Huk Kesehat. 2024;10(1):97–117. Available from: 10.24167/shk.v10i1.11542
10. Widiarta IN, Agung IG, Rwa M, Nyoman L, Aryani A. Harmonization of Regulations in Realizing Legal Certainty for the Protection of Medical Records and Personal Data. JLPH J Law, Polit Humanit. 2025;5(6):4463–70. Available from: 10.38035/jlph.v5i6
11. Laila MIK, Pribadi MSW, Ariyanto OS, Yunita PN, Rahayu SNT, Pujanggi WKA, et al. Faktor Penghambat Pelaksanaan Rekam Medis Elektronik di Rumah Sakit : Narrative Review. J Manaj Inf Kesehat Indones Vol. 2022;12(1):65–71. Available from: 10.33560/jmiki.v12i1.645%0AInformasi
12. Damayanti PS, Adiputra IMS, Pradnyantara IGANP. Tantangan penerapan Rekam Medis Elektronik (RME) berdasarkan regulasi Permenkes No. 24 Tahun 2022. Heal Sci Pharm J. 2025;9(1):47–55. Available from: 10.32504/hspj.v9i1.1164
13. Sidiq MA. Perlindungan Hukum terhadap Rumah Sakit atas Kebocoran Data Rekam Medik Elektronik yang Dilakukan oleh Peretas. Akad J Mhs Humanis. 2025;5(2):605–20.
14. Wihadi SP, Guntara P, Wibowo TAP. Perlindungan Hukum Bagi Rumah Sakit atas Pembukaan Data Rekam Medis Melalui Aplikasi SATU SEHAT. LABEL Law, Accounting, Business, Econ Lang. 2025;2(1):528–39.
15. Kementerian Kesehatan Republik Indonesia. Kebijakan Perlindungan Data Pribadi di Kementerian Kesehatan. Jakarta: Kementerian Kesehatan Republik Indonesia; 2020.
16. Dzikrah R. Evaluasi Implementasi SATUSEHAT sebagai Sistem Interoperabilitas Data Kesehatan di Indonesia: Kajian Literatur. ResearchGate. 2025;
17. Humas Badan Kebijakan Pembangunan Kesehatan. Kemenkes Integrasikan Ratusan Aplikasi Menuju Era SATUSEHAT [Internet]. Kabar BKPK. 2025. Available from: https://www.badankebijakan.kemkes.go.id/kemenkes-integrasikan-ratusan-aplikasi-menuju-era-satusehat/
18. Kementerian Kesehatan Republik Indonesia. Peta Jalan SATUSEHAT SDMK 2025-2029. Jakarta: Kementerian Kesehatan Republik Indonesia; 2025.
19. Badan Siber dan Sandi Negara (BSSN) RI. Peraturan Badan Siber dan Sandi Negara Republik Indonesia Nomor 8 Tahun 2024 tentang Standar dan Tata Cara Pelaksanaan Audit Keamanan Sistem Pemerintahan Berbasis Elektronik. Jakarta: Kementerian Kesehatan Republik Indonesia; 2024.