WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

Legal Protection of Patients' Confidentiality in the Era of Mandatory Electronic Medical Records

Winona May Hendrata[a], Asma Karim[b]
[a] Fakultas Hukum Ilmu Sosial dan Ilmu Politik, Universitas Terbuka, Tangerang. E-mail: winonamayh@gmail.com
[b] Fakultas Hukum, Universitas Widya Mataram, Yogyakarta. E-mail: asmak2261@gmail.com

Abstract

Electronic medical records (EMR) is the result of technology and information advancement in healthcare. However, the implementation of EMR has not been optimal, thus doubts about patient's data security inevitably rise. The method used in this research is statute approach specifically on Health Ministerial Regulation No. 24/2022, ITE Law, and PDP Law, as well as related empirical evidence. Implementation of EMR is obligated through the enactment of Indonesian Health Ministerial Regulation number 24 of 2022. The obligation to guard professional secret is regulated in legal enactment, as well as within health professionals code of ethics. EMR system with adequate requirement is crucial in order to guarantee the security of the data contained. As an electronic system under Indonesian law, EMR qualify for protection under Penal Code (KUHP) Article 332, which criminalizes unauthorized access to computer systems with penalties for breaching security protocols. The EMR system requirement has been regulated within the Health Ministerial Regulation, however more detailed technical explanation is still needed. The study proposes urgent regulatory harmonization, recommending strengthening the direct regulation of EMR to establish tiered access controls, synchronize the EMR regulation with BSSN security standards for health data, and a dedicated health data oversight body. This research contributes the first systematic analysis of EMR implementation under Indonesia's PDP Law, offering actionable policy solutions to balance care quality and data protection.

Keywords: *electronic medical records; health law; patient confidentiality*

A. Introduction

The digital era has driven significant transformations across various sectors, including healthcare. One notable change is the adoption of Electronic Medical Records (EMRs), which is now being implemented in many countries.[1] However, concerns remain regarding the challenges and legal issues that arise, particularly concerning the protection of patient data confidentiality. A medical record contains sensitive information about an individual, namely a patient, such as medical history, test results, and other personal information.[2] The leakage of this information could compromise patient privacy, expose vulnerabilities to unauthorized parties, and potentially endanger patients' lives.

Prior to the enactment of the omnibus law, Law No. 17 of 2023 on Health, the Ministry of Health issued Ministerial Regulation No. 24 of 2022, which mandates all healthcare facilities in Indonesia to implement EMRs as the primary medical record system. The legal status of EMRs has been further strengthened with the enactment of the omnibus law, Law No. 17 of 2023 on Health.

[1] Md. Khalid Hossain et al., *An exploratory study of electronic medical record implementation and recordkeeping culture: the case of hospitals in Indonesia*, *BMC Health Services Research*, Vol. 25 No. 1, February 2025, p. 249.
[2] Phyllis T. Floyd et al., *Defining the medical record: relationships of the legal medical record, the designated record set, and the electronic health record*, *Perspectives in Health Information Managemen*, Vol. 18 No. 4, 2021, p. 1h.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

These regulations provide clear definitions and frameworks for EMR. According to Article 1 paragraph 1 of Minister of Health Regulation No. 24 of 2022, a medical record is a document containing patient identification data, examinations, treatments, procedures, and other services provided to the patient. Meanwhile, Article 1 paragraph 2 explains electronic medical records as records created using an electronic system intended for medical record management.

The implementation of EMRs is expected to bring numerous benefits, such as improving the efficiency and quality of healthcare services. The adoption of EMR has been widely studied, with empirical evidence highlighting both its benefits and risks. A systematic review by Uslu and Stausberg (2021) analyzed 23 studies published between 2010 and 2019, predominantly from the United States, to evaluate the impact of EMRs on hospital care. Their findings reveal that EMRs significantly improve the quality of care, with 78% of studies (18/23) demonstrating positive effects, such as enhanced guideline adherence, reduced medication errors, and better coordination of patient care.[3] One study observed a significant 14% reduction in medication errors following EMR implementation.[4] These studies' results underscore EMR potential to enhance both clinical and operational efficiency of healthcare.

However, with digitization and the use of information technology, the risks of privacy breaches and data leaks may increase. One of the factors that increase the risk includes medical record information in EMRs can be accessed by multiple users simultaneously, unlike paper-based records, which typically exist in a single physical copy.[5] Therefore, the confidentiality and security of this data are of utmost importance.

Information contained in medical records is considered medical confidentiality, the secrecy of which is protected by law. The right to privacy is one of the righs explained on article 17 of International Covenant on Civil and Political Rights (ICCPR), which has been ratified based on Law no 12 of 2005 regarding the Ratification of International Covenant on Civil and Political Rights.

[3] Aykut Uslu & Jürgen Stausberg, *Value of the Electronic Medical Record for Hospital Care: Update From the Literature*, *Journal of Medical Internet Research*, Vol. 23 No. 12, December 2021, p. e26323.
[4] J. A. Zlabek, J. W. Wickus, & M. A. Mathiason, *Early cost and safety benefits of an inpatient electronic health record*, *Journal of the American Medical Informatics Association*, Vol. 18 No. 2, March 2011, pp. 169–172.
[5] Ming-Ling Sher et al., *Compliance With Electronic Medical Records Privacy Policy: An Empirical Investigation of Hospital Information Technology Staff*, *INQUIRY: The Journal of Health Care Organization, Provision, and Financing*, Vol. 54, January 2017, p. 0046958017711759.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

While existing studies demonstrate EMR benefits, few examine how Indonesia's legal framework addresses emerging digital challenges in healthcare confidentiality. This gap necessitates thorough examination of current regulations.

It is essential to thoroughly examine existing regulations and laws concerning the protection of patient data confidentiality in the era of EMRs, considering that EMRs are a relatively novel development to most parties in Indonesia. Whithin regulations and laws, it is crucial to clearly define the parties responsible in case of a breach of patient data confidentiality, how data should be stored and accessed, and the legal sanctions for violators. Additionally, existing laws should ensure a sense of security for healthcare professionals in their work. Strong legal protection can also instill confidence in patients seeking medical treatment, knowing that data confidentiality and patient privacy rights are guaranteed by law.[6]

This legal research examines Indonesia's regulatory framework for protecting patient data confidentiality in Electronic Medical Records (EMRs), with a focus on the Personal Data Protection (PDP) Law (No. 27 of 2022), Minister of Health Regulation No. 24 of 2022 on Medical Records, and relevant provisions of the Criminal Code (KUHP) using normative legal approach. The findings aim to provide actionable recommendations for policymakers, healthcare providers, EMR vendors, and patients to strengthen data security while balancing accessibility and compliance.

B. Research Method

This legal research uses normative judicial research methodswith a statutory approach focusing on the analysis of laws and regulations governing the confidentiality of patient data in the context of mandatory EMR implementation.[7] This research examines positive legal provisions regarding the protection of patient data confidentiality in the era of mandatory EMR. In addition, a conceptual and philosophical approach is employed to examine the underlying principles of medical confidentiality and patient privacy rights, especially in light of emerging data protection standards.

This research examines positive law regarding the protection of patient data confidentiality in the era of mandatory EMR. The materials used in this legal research include secondary data which includes primary legal materials and secondary legal materials. Primary legal materials, such as statutes and ministerial regulations, serve as the core sources for legal

[6] Yudi Yasmin Wijaya, Edy Suyanto, & Fanny Tanuwijaya, *Rekam Medis: Penggunaan Informasi Medis Pasien dalam Pelaksanaan Asas Perlindungan Publik*, *Veritas et Justitia*, Vol. 6 No. 2, December 2020, pp. 399–423.
[7] Ahamad Rosidi, M Zainuddin, & Ismi Arifiana, *Metode Dalam Penelitian Hukum Normatif Dan Sosiologis (Field Research)*, *Journal Law and Government*, Vol. 2 No. 1, February 2024, p. 46.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

analysis. Secondary legal materials including scholarly articles, legal commentaries, and jurisprudence are used to interpret and contextualize the statutory provisions.

Primary Legal Materials, namely legal materials consisting of statutory regulations:

1) Law Number 17 of 2023 concerning Health (hereinafter referred to as the Health Law)
2) Law Number 1 of 2023 concerning the Criminal Code (hereinafter referred to as the Criminal Code)
3) Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (hereinafter referred to as the ITE Law)
4) Law Number 27 of 2022 concerning Personal Data Protection (hereinafter referred to as the PDP Law)
5) Minister of Health Regulation number 24 of 2022 concerning Medical Records (hereinafter referred to as Minister of Health Regulation 24/2022)
6) Minister of Health Regulation number 36 of 2024 concerning Medical Secrets (hereinafter referred to as Minister of Health Regulation 36/2024)
7) Minister of Communication and Information Regulation number 20 of 2016 concerning Protection of Personal Data in Electronic Systems (hereinafter referred to as Minister of Communication and Information Regulation 20/2016)
8) National Cyber and Crypto Agency regulation number 4 of 2021 concerning Guidelines for Information Security Management of Electronic-Based Government Systems and Technical Standards and Procedures for Security of Electronic-Based Government Systems

Secondary legal materials includes textbooks, legal dictionaries and legal journals, and comments on court decisions. Legal materials were collected through library research using both printed and electronic sources. The analysis is conducted through statutory interpretation, employing grammatical, systematic, and teleological methods to determine the scope and adequacy of the legal framework.

C. Results and Discussion

1. Legal Position of Electronic Medical Record

Medical records are documents that contain information about an individual's identity, health status, and medical treatment history when accessing healthcare facility services. This

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

individual of interest is legally designated as a "patient" in this context.[8] The implementation of medical records is a legal obligation of healthcare facilities, as stipulated in Law No. 17 of 2023 Article 173 paragraph (1) letter c.

In healthcare practice, implementing medical records is essential for the patient's treatment, as the patient's health and treatment history are vital information required for providing healthcare services to the patient.

Medical records have several important functions in the health sector. The functions of medical records include:[9,10]

1. Facilitating written communication among healthcare professionals involved in providing care, treatment, and services to patients.
2. As a basis for planning the care to be provided to a patient.
3. Providing written evidence of all services, disease progression, and treatment received by a patient during their visit or stay at a healthcare facility.
4. As a basis for analyzing the quality of care provided to patients within a healthcare facility.
5. Protecting the legal interests of patients, healthcare facility institutions, and healthcare professionals.
6. As a specific data source for research and educational purposes.
7. As a basis for calculating medical service costs for patients.
8. As a basis for insurance claims for both healthcare facilities and patients.
9. As a basis for planning, marketing, and promoting healthcare facilities.
10. Providing health statistics data.

The complexity of the functions outlined above in medical records is one of the reasons why there is a need for the upgrade of medical record systems to EMRs.[11] Given the multi-dimensional functions mentioned, medical records contain various data, including personal data, health status, and a patient's medical history. The content of medical records in accordance with Minister of Health Regulation No. 24/2022, as stipulated in Article 26 paragraph (6), should at least include the patient's identity; results of physical and supporting

[8] Thalia Prameswari & Wahyu Andrianto, *Pasien: Konsumen Yang Unik*, *Jurnal Hukum Kesehatan Indonesia*, Vol. 1 No. 02, April 2022, pp. 132–139.
[9] Novekawati, 2019, *Hukum Kesehatan*, Sai Wawai Publishing: Semarang, pp 63-4.
[10] Tiromsi Sitanggang, 2019, *Aspek Hukum Kepemilikan Rekam Medis Terhadap Perlindungan Hak Pasien*, Penerbit Yayasan Kita Menulis: Medan, pp 5-6.
[11] Naresh Khatri, *Effective implementation of electronic medical records and health information technologies*, *Missouri Medicine*, Vol. 112 No. 1, 2015, pp. 41–45.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

examinations; diagnosis, treatment, and follow-up healthcare service plans; and the name and signature of the healthcare professional providing the healthcare service. This data elements coincides with the personal data outlined in PDP Law article 4, where health information falls under specific personal data, and identity falls under general personal data.

Therefore, the information contained in medical records falls within the realm of privacy rights and is highly sensitive. An individual's health status can be linked to many aspects that have the potential to harm that individual. Information within medical records known to unauthorized parties can affect others' perceptions of an individual's capabilities, reveal physical weaknesses, influence social perceptions, and have other detrimental impacts if the individual's confidential information is disclosed.[12] Furthermore, the accuracy of the content in medical records significantly impacts various aspects such as treatment planning, healthcare service quality evaluation, financing, and legal evidence.[13]

It is explicitly stated that medical records are the property of healthcare facilities (Minister of Health Regulation No. 24/2022, Article 25), while the content of medical records belongs to the patient (Minister of Health Regulation No. 24/2022, Article 26). Although the content of medical records belongs to the patient, under certain circumstances, third parties such as insurance companies, law enforcement, and the judiciary may access the content of medical records. Therefore, ownership of the content of medical records can be considered public, albeit with access restricted by law.[14]

Healthcare facilities are also required to grant access to the entire content of a patient's EMR to the Ministry of Health (Minister of Health Regulation No. 24/2022, Article 28) for health data management purposes. The disclosure of medical record data must be done with the approval of the Minister or upon a court order (Minister of Health Regulation No. 24/2022, Article 36).

This dual ownership model creates tension with PDP Law Article 7, which grants data subjects exclusive rights to access and obtains copy of personal data. However, the healthcare

---

[12] Stevanus Passat & Evita Israhadi, *Confidentiality of Medical Record as Legal Protection of Patient's Privacy Rights*, *Proceedings of the 1st International Conference on Law, Social Science, Economics, and Education, ICLSSEE 2021, March 6th 2021, Jakarta, Indonesia*, presented at the Proceedings of the 1st International Conference on Law, Social Science, Economics, and Education, ICLSSEE 2021, March 6th 2021, Jakarta, Indonesia, Salatiga, Indonesia, EAI, 2021

[13] Ida Sugiarti, *Legal Protection of Patient Rights to Completeness and Confidentiality in Management of Medical Record Documents*, *The Proceedings of the 2nd Bakti Tunas Husada-Health Science International Conference (BTH-HSIC 2019)*, presented at the 2nd Bakti Tunas Husada-Health Science International Conference (BTH-HSIC 2019), Tasikmalaya, Indonesia, Atlantis Press, 2020

[14] Tiromsi Sitanggang, 2019, *Aspek Hukum Kepemilikan Rekam Medis Terhadap Perlindungan Hak Pasien*, Penerbit Yayasan Kita Menulis: Medan, p 4.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

regulations create operational ambiguities: they neither specify timelines for fulfilling patient access requests nor reconcile the Ministry of Health's broad access rights (Article 28) with PDP Law's consent requirements. Most critically, the medical record framework lacks explicit exceptions for the PDP Law's right to erasure (Article 8), despite legitimate needs to retain treatment histories for clinical and legal purposes. This regulatory misalignment risks violating PDP Law Article 2(1)'s mandate for sectors to conform to its standards, potentially exposing healthcare providers to legal challenges when denying patient requests based solely on Ministry of Health provisions. The necessity for regulatory harmonization in the context of patient data protection has been identified as a critical focus in numerous scholarly studies.[15]

The obligation to utilize EMRs is reinforced by the enactment of the Omnibus Health Law, Law No. 17 of 2023 concerning Health, specifically in the explanation of Article 173 paragraph (1) letter c. Article 173 stipulates the obligation of healthcare facilities, where paragraph (1) letter c states that healthcare facilities must maintain medical records. In the explanation of this article, the term "Medical Records" refers to electronic medical records. The use of non-electronic medical record systems is limited to situations where there are still obstacles in implementing electronic medical records systems. As of now, many hospitals and healthcare facilities in Indonesia are facing challenges in implementing electronic medical records.[16] These challenges need to be addressed promptly as they have implications for the legal protection of medical record data.

2. Challenges in ERM Implementation and Medical Record Data Protection

The adoption of EMRs represents a transformative shift in healthcare documentation, offering significant advantages over conventional paper-based systems. However, this transition introduces multifaceted challenges across technical, operational, legal, and human resource dimensions that healthcare institutions must strategically address. As Indonesia mandates EMR implementation through Ministerial Regulation No. 24 of 2022, healthcare facilities confront critical barriers ranging from infrastructure readiness and workforce adaptation to data security compliance and third-party risk management. These

[15] Britt E. Bente et al., *eHealth implementation in Europe: a scoping review on legal, ethical, financial, and technological aspects*, *Frontiers in Digital Health*, Vol. 6, March 2024, p. 1332707.; Jenifer Sunrise Winter & Elizabeth Davidson, *Harmonizing regulatory regimes for the governance of patient-generated health data*, *Telecommunications Policy*, Vol. 46 No. 5, June 2022, p. 102285.

[16] Tirsa Sharon Tilaar & Pan Lindawaty Suherman Sewu, *Review of Electronic Medical Records in Indonesia and its Developments Based on Legal Regulations in Indonesia and its Harmonization with Electronic Health Records (Manual for Developing Countries)*, *Daengku: Journal of Humanities and Social Sciences Innovation*, Vol. 3 No. 3, April 2023, pp. 422–430.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

implementation challenges, if unresolved, may compromise the anticipated benefits of EMR systems while potentially jeopardizing patient data protection and healthcare service quality. The following analysis examines these barriers through four key lenses: technical infrastructure requirements, human resource capacity, legal accountability frameworks, and system security.

Technical and Infrastructure Issue

The EMR system as an electronic system requires continuous maintenance and updates. Maintenance and updates are related to smooth operation, security, and compatibility with other devices.[17] The EMR storage system must ensure the security, integrity, confidentiality, and availability of EMR data (Minister of Health Regulation 24/2022 article 20). With these provisions, both hardware and software facilities for EMR storage must have specific specifications. Data security equipment should also include protection against breaches such as firewalls, antivirus software, and intrusion detection software.[18] These specifications should be regulated by law as minimum specifications for the EMR system.

The implementation of EMR can reduce the economic burden in the healthcare sector. The obligation of EMRs implementation for healthcare facilities certainly requires a large procurement fund.[19] Until now, many hospitals and healthcare facilities in Indonesia are still constrained by the expensive procurement of infrastructure for electronic medical records. This infrastructure includes hardware, software, and human resources.[20]

Human Resource Readiness and Training

The shift from paper-based systems to electronic systems in healthcare requires healthcare professionals to adapt to the new electronic system for medical record keeping. Documentation in medical records during the healthcare service process by healthcare professionals is typically part of the standard operating procedures (SOP) for service delivery.[21] Healthcare providers must learn to input patient data by typing rather than

[17] Roboam R Aguirre et al., *Electronic Health Record Implementation: A Review of Resources and Tools*, *Cureus*, September 2019
[18] Fouzia F. Ozair et al., *Ethical issues in electronic health records: A general overview*, *Perspectives in Clinical Research*, Vol. 6 No. 2, 2015, pp. 73–76.
[19] Kim-Huong Nguyen et al., *Economic evaluation and analyses of hospital-based electronic medical records (EMRs): a scoping review of international literature*, *Npj Digital Medicine*, Vol. 5 No. 1, March 2022, p. 29.
[20] Tilaar, "Review of Electronic Medical Records," 4748-4769.
[21] Addisalem Workie Demsash et al., *Health professionals' routine practice documentation and its associated factors in a resource-limited setting: a cross-sectional study*, *BMJ Health & Care Informatics*, Vol. 30 No. 1, February 2023, p. e100699.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

writing.[22] This transition process is closely tied to each individual's technological awareness, leading to potential variations in implementation among personnel.

Inputting EMR data are the responsibility of each health professional who provides care (Minister of Health Regulation 24/2022 article 15). The adoption of EMR systems can potentially disrupt workflow in healthcare facilities.[23] Comprehensive training is essential for standardizing the implementation of EMRs and enhancing personnel's ability to operate them.[24] Evaluation of the quality, consistency, and completeness of EMR documentation is necessary during this transition.

Medical records and documentation are crucial as they serve as a reference for healthcare professionals in their work and in providing subsequent care. For instance, medical records are essential for recording a patient's history of drug allergies. Without proper documentation of drug allergies, there is a risk of healthcare professionals inadvertently administering the same medication that the patient is allergic to. Administering medication to a patient with a known drug allergy can trigger varying allergic reactions, some of which may be severe or fatal. Therefore it is crucial for healthcare professionals to ensure the completeness and accuracy of EMR documentation to protect themselves legally in their medical practice. Interface design, interoperability, and inability to track test result impacts diagnostic accuracy on the use of EMR.[25]

Legal Risk and Thid Party Accountability

According to Ministerial Regulation 24 of 2022, EMRs can be developed by each healthcare facility independently or in collaboration with vendors providing EMR applications or platforms. Both approaches to EMR implementation present their own challenges in practice.

Unlike conventional medical records, the adoption of EMR systems requires expertise in information technology due to the complexity of information systems. If healthcare facilities engage third-party personnel in managing EMRs, there is involvement of external parties related to the EMR. The involvement of third parties also poses a risk of patient data

[22] Anzany Tania Dwi Putri, *Challenges in implementing electronic medical record in Indonesia healthcare facilities*, *Jurnal Medika Hutama*, Vol. 4 No. 03, n.d., pp. 3427–31.
[23] Dean F. Sittig & Hardeep Singh, *Rights and responsibilities of users of electronic health records*, *Canadian Medical Association Journal*, Vol. 184 No. 13, September 2012, pp. 1479–1483.
[24] Raed Abdullah Alharbi, *Adoption of electronic health records in Saudi Arabia hospitals: Knowledge and usage*, *Journal of King Saud University - Science*, Vol. 35 No. 2, February 2023, p. 102470.
[25] Ram A. Dixit et al., *Electronic Health Record Use Issues and Diagnostic Error: A Scoping Review and Framework*, *Journal of Patient Safety*, Vol. 19 No. 1, January 2023, pp. e25–e30.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

breaches, which some studies has considered third-party access a threat.[26] Minister of Health Regulation have addressed this threat, where the third party EMR vendor are prohibited from disclosing, extracting, manipulating, damaging, exploiting data, or engaging in any other actions detrimental to Healthcare Facilities. These limitation should be recorded in a non disclosure agreement between the EMR provider and the healthcare facility (Minister of Health Regulation 24/2022 article 22). However other than the non-disclosure agreement, no other mechanism limitting third party's access to EMR systems were elaborated.

The EMR storage system, either independently maintained or by collaboration with a third party must ensure the security, integrity, confidentiality, and availability of Electronic Medical Record data (Minister of Health Regulation 24/2022 article 20). Providing backup is also mandatory according to article 20(4). Therefore, safeguarding patient confidentiality is also the responsibility of the vendor providing the EMR system.

These security gaps directly impair the constitutional right to privacy under Article 28G of the Indonesian Constitution and undermine protections under the PDP Law. Three critical vulnerabilities emerge: (1) patients lack legal recourse when vendors experience data breaches but face no mandatory disclosure obligations; (2) third parties unlawfully access data beyond treatment purposes, violating the purpose limitation principle under PDP Law Article 20; and (3) system failures generate documentation errors that compromise care quality without established accountability mechanisms. Furthermore, the right to erasure (PDP Law Article 8) is rendered ineffective when vendors or healthcare retain backup copies indefinitely, lacking transparent retention policies that align with the storage limitation principle. This regulatory vacuum creates systemic risks where patients cannot exercise fundamental data rights despite statutory guarantees.

System Security and Regulatory Compliance

Security is greatly influenced by the processes mentioned above, and security is an important component of efforts to protect medical record data, one of which is patient data. Therefore, maintenance of the EMR system should be optimal at all times. The transition of conventional health record to EMR represents a significant advancement in the healthcare

[26] Zongda Wu et al., *How to ensure the confidentiality of electronic medical records on the cloud: A technical perspective*, *Computers in Biology and Medicine*, Vol. 147, August 2022, p. 105726.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

field. Unlike conventional paper-based medical records that are handwritten, EMRs are digital and stored electronically.[27]

Screening challenges to the implementation of EMR is part of protecting patient data confidentiality in EMR. In addition to requiring ethics and knowledge from access rights holders, EMR system must also be able to withstand external threats. A study revealed that system architectural issue and credential misuse are the main threat to EMR security, and hacking activity most often target these vulnerable points.[28] The strategies to mitigate these vulnerabilities include user authentication and authorization system, blockchain, encryption, and session passwords.[29]

3. EMR Access Regulation

The confidentiality of the contents of EMR also depends on the individuals who are granted access to EMR, so regulations related to access rights are also a major consideration in confidentiality protection. The system's ability to restrict access to EMR is one of the characteristics of EMR information systems found in various countries that use health information systems. For example, National Health Services (NHS) of United Kingdom utizilize smartcard system with biometric authentication.[30]

Some EMR implementations use a user access system. In short, this system provides access to each individual who typically can be accessed by a username and password known only to the access owner. Usually, this access is related to the name and profession of the access owner.[31] In the ITE Law, this password is known as an access code in Article 1 point 16 of the ITE Law. The implication of this system is that the identity of the person who fills in certain data at a certain time can be known, so this user access is like a "signature" in filling out EMR. Ths access code system is also the required system as regulated in Minister of Health Regulation 24/2022 article 30.

In Minister of Health Regulation No. 24 of 2022 Article 13, the authority of each healthcare profession in filling out EMR has been detailed. This division of authority is

---

[27] Dian Wijayanti, Erik Iman Heri Ujianto, & Rianto Rianto, *Uncovering Security Vulnerabilities in Electronic Medical Record Systems: A Comprehensive Review of Threats and Recommendations for Enhancement*, *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, Vol. 10 No. 1, February 2024, p. 73.
[28] *Ibid.*
[29] *Ibid.*
[30] Tzu-Wei Lin et al., *A Smartcard-Based User-Controlled Single Sign-On for Privacy Preservation in 5G-IoT Telemedicine Systems*, *Sensors (Basel, Switzerland)*, Vol. 21 No. 8, April 2021, p. 2880.
[31] Usha Nicole Cobrado, Suad Sharief, Noven Grace Regahal, Erik Zepka, Minnie Mamauag, & Lemuel Clark Velasco, *Access control solutions in electronic health record systems: A systematic review, Informatics in Medicine Unlocked,* vol. 49, 2024, p. 101552.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

closely related to the access of each medical personnel to patient data. For example, only doctors providing healthcare services can fill out a patient's medical history. Therefore, user access belonging to the doctor is regulated to be used for filling out the patient's medical history, while user access belonging to administrative staff cannot access or fill out medical histories.

The username and password of user access must be known solely by each owner. The goal is to prevent confusion of the data filler's identity and limit access to the contents of EMR. However, it is not uncommon to find negligence in implementation that allows user access to be used by someone other than the owner.[32] For example, the practice of displaying user credentials in clinical workspaces constitutes a form of negligence that exposes sensitive health data to unauthorized access. This action can allow unauthorized individuals to access the EMR information system, even if they do not intend to disclose data.[33] Credential misuse has been identified as one of the most common threat to EMR security.[34] This can create an opportunity for the leakage of patient's confidential information. Negligence like this should be prevented by increasing knowledge of the EMR system and awareness of the legal consequences in operating EMR.

The access code system aligns partially with PDP law principles, however there are still gaps in which purpose limitation and data minimization principle of PDP law has not been adressed. The management of personal data must be limited to a certain purpose, therefore access broaness must be limited to ensure patient data are used only for treatment needs. There are also lack of enforcement mechanism against personal data internal misuse. Furthermore, no explicit penalites exist for credetial sharing between authorized users.

Access codes are generally protected by law, specifically under Article 332 of the Indonesian Penal Code which states: (1) "Anyone intentionally and without right or unlawfully accesses another person's computer and/or electronic system by any means, shall be punished with imprisonment for a maximum of 6 (six) years or a fine of up to category V. (2) Anyone intentionally and without right or unlawfully accesses a computer and/or electronic system by any means with the purpose of obtaining electronic information and/or electronic documents, shall be punished with imprisonment for a maximum of 7 (seven)

---

[32] Adil Hussain Seh et al., *Healthcare Data Breaches: Insights and Implications*, *Healthcare*, Vol. 8 No. 2, May 2020, p. 133.
[33] Metty Paul, Leandros Maglaras, Mohamed Amine Ferrag, & Iman Almomani. *Digitization of healthcare sector: A study on privacy and security concerns.* ICT Express, vol. 9, no. 4, 2023, pp. 571-588.
[34] D. Wijayanti, E.I.H. Ujianto, R. Rianto,*cited*

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

years or a fine of up to category V. (3) Anyone intentionally and without right or unlawfully accesses a computer and/or electronic system by violating, bypassing, exceeding, or breaking through security systems, shall be punished with imprisonment for a maximum of 8 (eight) years or a fine of up to category VI."

It is important to emphasize that one of the elements of the above paragraph is without right or against the law. This means that access rights regulations must be clearly defined in each healthcare facility.

According to the Indonesian Penal Code (KUHP) article 443, the disclosure of confidential information that must be kept due to position and profession is punishable by law. Article 443 paragraph (2) further explains that the prosecution of such criminal acts must be based on a complaint from the party whose confidentiality was breached. Administrative sanctions are also mentioned on Minister of Health Regulation 24/2022 article 43, however the sanction for SOP non-compliance on healthcare professional individual are vague. The management of medical records is the obligation of healthcare facilities, therefore maintaining patient confidentiality and medical records is the responsibility of all individuals working in those healthcare facilities.[35]

Keeping patient confidentiality is a legal mandate and also part of the professional ethics of healthcare professionals.[36] Current regulations establish distinct accountability pathways for access violations. Healthcare workers who knowingly or negligently share access credentials face prosecution under KUHP Article 332(1) for unlawful system access, with penalties of up to six years' imprisonment, while KUHP Article 443 simultaneously enables patients to pursue complaint-based litigation for confidentiality breaches. For facility administrators, failure to implement adequate access SOPs triggers administrative sanctions under Minister of Health Regulation 24/2022 Article 30, though the regulation's silence on specific penalties creates enforcement uncertainties.

Access rights holders and facility administrator must understand the legal consequences of having access rights and realize that access rights must be safeguarded to the best of their ability. The allocation of access rights is the responsibility of healthcare facility leaders, which must be formalized in the form of regulations and standard operating procedures (SOP) (Minister of Health Regulation 24/2022, article 30).

---

[35] Ridwan Ridwan, *Pertanggungjawaban Hukum Pidana terhadap Pelanggaran Rahasia Medis*, *Jurnal Hukum & Pembangunan*, Vol. 49 No. 2, July 2019, p. 338.
[36] Tiromsi Sitanggang, 2019, Aspek Hukum Kepemilikan Rekam Medis Terhadap Perlindungan Hak Pasien, Penerbit Yayasan Kita Menulis: Medan, p 5-6.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

4. The ITE Law and Data Protection in EMR Implementation

Law number 11 of 2008 concerning Electronic Information and Transactions (hereinafter referred to as the ITE Law) specifically regulates electronic information and transactions, where electronic systems fall within its scope. According to Article 1 paragraph 5, an electronic system is a series of electronic devices and procedures that function to prepare, collect, process, analyze, store, display, announce, send, and/or disseminate electronic information. This definition has been explicitly adopted by Minister of Health Regulation 24/2022 for medical records. This legal synergy confirms EMRs' status as protected "electronic documents" under ITE Law Article 1(4), granting them equivalent evidentiary validity to paper records per Article 5(1).

The ITE Law as a legal product is a tool of state control over information and electronic systems.[37] The development of ITE and its increasing integration into society necessitates clear legal regulations to regulate information exchange in the digital world. The enforcement of new and up-to-date regulations is needed because technological advancements are also accompanied by the emergence of new criminal activities. These criminal activities can be referred to as cybercrime. Cybercrime is a crime against computer systems or networks and crimes that utilize computer means.[38]

Patient data can be a target of cybercrime. The public is increasingly vigilant against cybercrime, so data security is often considered when providing personal data into a system.[39] The lack of assurance in confidentiality and privacy protection can result in a decrease in public trust in the implementation of EMR, which can ultimately impact public trust in the healthcare system as a whole. During the COVID-19 pandemic, the government launched the electronic Health Alert Card (eHAC) platform, which is mandatory for international travel purposes. This system stores user identity data as well as travel history and COVID-19 test history. The platform was once suspected of experiencing a data breach.[40] The eHAC platform incident demonstrated how health data vulnerabilities can erode public trust. This phenomenon has been extensively documented in studies on government-managed systems, demonstrating that cybersecurity breaches can erode public trust not only in the affected

[37] Radita Setiawan & Muhammad Okky Arista, *Efektivitas Undang-Undang Informasi dan Transaksi Elektronik di Indonesia dalam Aspek Hukum Pidana*, *Recidive*, Vol. 2 No. 2, 2013, pp. 139–146.
[38] Muhammad Anthony Aldriano & Mas Agus Priyambodo, *Cyber Crime dalam Sudut Pandang Hukum Pidana*, *Jurnal Kewarganegaraan*, Vol. 6 No. 1, June 2022
[39] Ying He et al., *Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review*, *Journal of Medical Internet Research*, Vol. 23 No. 4, April 2021, p. e21747.
[40] Amir Nabbilah, *Legal Protection of Patient Data Confidentiality Electronic Medical Records*, *Soepra Jurnal Hukum Kesehatan*, Vol. 5 No. 2, n.d., pp. 198–208.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

platform but also in broader governmental institutions.[41] Data security issues like this need to be prevented to avoid undermining public trust in electronic systems, especially those organized by the government.

One of the regulations derivated from the ITE Law is Minister of Communication and Information Regulation No. 20 of 2016 concerning the Protection of Personal Data in Electronic Systems. Ministerial Regulation 20/2016 establishes a critical framework for personal data protection by: (1) imposing strict liability on electronic system providers for protection failures (Article 28(c)); (2) requiring authorization for any collection, processing, or dissemination of personal data (Article 36(1)); and (3) mandating administrative sanctions for violations.

However, three key limitations emerge in its application to healthcare data: first, the regulation fails to account for the heightened sensitivity of medical information under PDP Law Article 4(1); second, its generic breach notification timelines (Article 26(3)) disregard clinical urgency; and third, it lacks sector-specific technical standards for health data encryption. These gaps persist despite Minister of HEalth Regulation 24/2022's recognition of EMRs as protected electronic systems, creating regulatory fragmentation that necessitates lex specialis provisions to address healthcare's unique data protection requirements.[42]

The sanctions for the failure to protect personal data for information system providers need to be clarified whether there is a difference between general information system providers and those providing EMR, as personal data in EMR is part of medical record data with restricted access, and unauthorized access is punishable by law. Therefore, it is necessary to further study the need for specific provisions that are *lex specialis* applied to EMR system providers.

5. Electronic Medical Record Integration with SATUSEHAT Platform and its legal protection

The Ministry of Health mandates that electronic medical record systems must be integrated with the SATUSEHAT platform, which is the Ministry of Health's national health data integration system. The mandatory system compatibility for intoperability with a national platform is regulated on Minister of Health Regulation 24/2022 article 8 and 10.

[41] Ryan Shandler & Miguel Alberto Gomez, *The hidden threat of cyber-attacks – undermining public confidence in government*, *Journal of Information Technology & Politics*, Vol. 20 No. 4, October 2023, pp. 359–374.; Saman Iftikhar, *Cyberterrorism as a global threat: a review on repercussions and countermeasures*, *PeerJ. Computer Science*, Vol. 10, 2024, p. e1772.

[42] Afiif Hadiani Pratiwi, Edi Wahjuni, & Nuzulia Kumala Sari, *Perbuatan Melawan Hukum dalam Kebocoran Data Penumpang Lion Air Group*, *Journal of Private and Economic Law*, Vol. 1 No. 2, n.d., pp. 107–134.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

Article 22 of the same regulation mandates compulsory interoperability for all electronic medical record systems. Integration of health data with SATUSEHAT was established through Minister of Health Decree no HK.01.07/MENKES/133/2023 concerning National Health Data Integration Through SATUSEHAT. However, Minister of Health Regulation No. 24 of 2022 does not explicitly mention the SATUSEHAT platform, creating a regulatory gap in governing the technical standards and legal liabilities for this specific national health data integration system

SATUSEHAT is a platform that connects systems and integrates individual health data across healthcare facilities. Integration of local EMR with a national platform is nescesaary to enable health information exchange in order to integrate patient care across health facilities, in which successful integration has been related to higher quality of care.[43] Integration of EMR with national platform place the government as a party responsible in protecting patient's health data.

This integration necessitates robust cybersecurity measures tailored to health data systems, including comprehensive preventive measure compliant with PDP Law Article 39(1), comprehensive audit per Minister of Health Regulation 24/2022 Article 20(2), and security protocols meeting BSSN's standard for government system based on BSSN regulation 4/2021. Cybersecurity is a practice to protect computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.[44]

SATUSEHAT platform is a state-owned information system, so breaches into the state information system are specifically protected by law, separate from regular information systems. The legal framework establishes a tripartite accountability structure: hospitals bear primary responsibility for ensuring functional integration (Minister of Health 24/2022 Article 19), vendors must maintain system security under ITE Law Article 34(3), while the Ministry of Health oversees compliance through PDP Law Article 58 monitoring mechanisms.

Under PDP Law Article 46, personal data controllers must disclose breach details to both affected data subjects and authorities within 72 hours of discovery. For EMR systems integrated with SATUSEHAT, this obligation creates shared liability among three potential controllers: (1) healthcare facilities as primary data collectors (Minister of Health Regulation

[43] A Jay Holmgren et al., *Health Information Exchange: Understanding the Policy Landscape and Future of Data Interoperability*, *Yearbook of Medical Informatics*, Vol. 32 No. 01, August 2023, pp. 184–194.
[44] Eko Budi, Dwi Wira, & Infantono Ardian, *Strategies For Strengthening Cyber Security To Achieve National Security in Society 5.0*, *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia - Akademi Angkatan Udara*, Vol. 3, 2021, pp. 223–234.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

24/2022 Article 25), (2) EMR vendors managing cloud infrastructure (Minister of Health Regulation 24/2022 Article 2), and (3) the Ministry of Health as SATUSEHAT operator. Current regulations lack clear delineation of these layered responsibilities, necessitating amendments to MoH Regulation 24/2022 to specify notification sequencing among parties, standardized breach assessment criteria for health data, and exemptions for cases where disclosure may impede ongoing forensic investigations.

Essentially, the SATUSEHAT platform fulfills the elements of (1) an electronic system, (2) owned by the government, and (3) information that must be kept confidential or protected, therefore one of the legal protections for the SATUSEHAT platform is outlined in the Indonesian Criminal Code. Article 335 of the Indonesian Criminal Code (KUHP) stipulates a maximum prison sentence of 12 (twelve) years or a fine of the highest category VII for individuals who, without authorization, use or access a computer or electronic system in any way, with the intention of obtaining, altering, damaging, or removing information owned by the government that must be kept confidential or protected. This sanction operates concurrently with PDP Law Article 57's financial penalties of up to 2% annual revenue for negligent breaches. This layered legal protection framework combining KUHP Article 335's criminal sanctions for intentional breaches with PDP Law Article 57's administrative penalties for negligence creates a complementary enforcement mechanism that addresses both malicious cybercrimes and institutional security failures in protecting sensitive health data contained in SATUSEHAT platform. The implementation challenges underscore the need for clearer ministerial guidance on shared responsibility models, especially concerning legacy hospital systems requiring infrastructure upgrades to meet both SATUSEHAT integration requirements and the PDP Law's data minimization principles under Article 20.

A study has identified the characteristic of successful health information integration such as established in the UK's NHS and Poland's LIGHt (Local Interoperability Gateway for Healthcare) was the central strategic planning and involvement, which includes policy-making and enforcing.[45] Standardization of EMR and telemedicine in order to improve its capability to interoperate with a central system[46] should be enforced through policy. As a newly established platform, SATUSEHAT's interoperability should be governed by a

[45] A.J. Holmgren et al.,*cited*

[46] Putu Priyanka Sonia Dewi, Muharman Lubis, & Lukman Abdurrahman, *Aligning Healthcare Strategies Through Digital Information and Technology: Challenges and Solution*, *2024 12th International Conference on Cyber and IT Service Management (CITSM)*, presented at the 2024 12th International Conference on Cyber and IT Service Management (CITSM), Batam, Indonesia, IEEE, 2024, pp. 1–6.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

centralized national strategy that combines (1) mandatory technical standardization for all integrated EMR systems (including API protocols and data formats aligned with HL7/FHIR international standards), (2) strict policy enforcement mechanisms with BSSN-audited compliance checks, and (3) multi-stakeholder governance involving the Ministry of Health, healthcare providers, and digital health vendors.

D. Conclusion

The legal position and importance of implementing EMR for improving healthcare services in Indonesia has been clear and explicit, making the obligation to implement EMR in all healthcare facilities in Indonesia an absolute must. In order to uphold the privacy rights of Indonesian citizens, the law plays a crucial role in guiding the uniform implementation of EMR. Therefore, efforts are needed to identify obstacles in the implementation of EMR, especially those that have the potential to disrupt the protection of patient medical record data. Challenges in implementing medical records include the financial inability of healthcare facilities to provide adequate infrastructure, lack of healthcare professionals' ability to operate EMR, and the involvement of third parties in EMR implementation, increasing the risk of medical record data breaches.

This study demonstrates that Indonesia's EMR implementation faces three fundamental legal challenges: first, the tension between PDP Law's data minimization principle (Article 4(3)) and SATUSEHAT's comprehensive integration requirements creates systemic overcollection of health data; second, KUHP Article 335's focus on intentional breaches leaves negligent credential sharing unaddressed; and third, MoH Regulation 24/2022's technical mandates lack alignment with BSSN's cybersecurity standards (Regulation 4/2021), particularly regarding encryption protocols for sensitive medical records. These findings reveal critical regulatory gaps that prior studies have not analysed, namely the absence of sector-specific breach sanctions under PDP Law and ambiguous liability divisions between hospitals and vendors under ITE Law Article 34.

The alignment of legal regulations with the capabilities of healthcare facilities in the field is crucial for establishing a quality EMR system that can safeguard patient interests. To address these issues, urgent reforms should include: (1) amendments to MoH 24/2022 elaborating the multiple party responsibility that may consist of healthcare facility, EMR vendors, and government; (2) enforcement of cyber security and cybercrime mitigation standards for EMR, such as detailed by BSSN Regulation 4/2021 Article 12; and (3) establishment of a health data certification body to audit compliance. Urgent harmonization

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

between Electronic Medical Record (EMR) regulations and data protection laws, particularly in aligning MoH Regulation 24/2022's technical requirements with PDP Law principles, is critical to safeguard constitutional privacy rights and maintain public trust in Indonesia's healthcare digital transformation.

The obligation to implement EMR without optimal preparation may actually increases the risk of patient data leakage due to the involvement of multiple parties in EMR implementation compared to conventional medical records. Facilities with adequate minimum specifications need to be detailed in regulations, while also considering the financial capabilities of healthcare facilities. Additionally, the ability of healthcare professionals to operate EMR needs to be continuously improved. Screening challenges to EMR implementation are part of protecting patient data confidentiality in EMR. In addition to requiring ethics and knowledge from access rights holders, EMR infrastructure must also be robust to face external threats.

Legal protection should be felt before data leakage occurs. In addition to deterring criminals, regulations are needed to ensure data protection. The losses due to data leaks are difficult to measure and stop, as leaked personal data can be repeatedly misused. Even if data leakers are sanctioned or have compensated based on court decisions, the losses felt by those whose data is leaked can continue because leaked data outside is almost impossible to retrieve. Therefore, data leakage prevention must be implemented from the source.

BIBLIOGRAPHY

Abdullah Alharbi, Raed, "Adoption of electronic health records in Saudi Arabia hospitals: Knowledge and usage", Journal of King Saud University - Science, Vol. 35 No. 2, February 2023, P. 102470. DOI:10.1016/j.jksus.2022.102470.

Aguirre, Roboam R, Orlando Suarez, Mailenys Fuentes, Marcos A Sanchez-Gonzalez, "Electronic Health Record Implementation: A Review of Resources and Tools", Cureus, September 2019, P. . DOI:10.7759/cureus.5649.

Aldriano, Muhammad Anthony, Mas Agus Priyambodo, "Cyber Crime dalam Sudut Pandang Hukum Pidana", Jurnal Kewarganegaraan, Vol. 6 No. 1, June 2022, P. .

Bente, Britt E., Anne Van Dongen, Ruud Verdaasdonk, Lisette Van Gemert-Pijnen, "eHealth implementation in Europe: a scoping review on legal, ethical, financial, and technological aspects", Frontiers in Digital Health, Vol. 6, March 2024, P. 1332707. DOI:10.3389/fdgth.2024.1332707.

Budi, Eko, Dwi Wira, Infantono Ardian, "Strategies For Strengthening Cyber Security To Achieve National Security in Society 5.0", Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia - Akademi Angkatan Udara, Vol. 3, 2021, Pp. 223–234.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

Demsash, Addisalem Workie, Sisay Yitayih Kassie, Abiy Tasew Dubale, Alex Ayenew Chereka, Habtamu Setegn Ngusie, Mekonnen Kenate Hunde, Milkias Dugassa Emanu, Adamu Ambachew Shibabaw, Agmasie Damtew Walle, "Health professionals' routine practice documentation and its associated factors in a resource-limited setting: a cross-sectional study", BMJ Health & Care Informatics, Vol. 30 No. 1, February 2023, P. e100699. DOI:10.1136/bmjhci-2022-100699.

Dixit, Ram A., Christian L. Boxley, Sunil Samuel, Vishnu Mohan, Raj M. Ratwani, Jeffrey A. Gold, "Electronic Health Record Use Issues and Diagnostic Error: A Scoping Review and Framework", Journal of Patient Safety, Vol. 19 No. 1, January 2023, Pp. e25–e30. DOI:10.1097/PTS.0000000000001081.

Floyd, Phyllis T., Jim C. Oates, Julie W. Acker, Robert W. Warren, "Defining the medical record: relationships of the legal medical record, the designated record set, and the electronic health record", Perspectives in Health Information Managemen, Vol. 18 No. 4, 2021, P. 1h.

He, Ying, Aliyu Aliyu, Mark Evans, Cunjin Luo, "Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review", Journal of Medical Internet Research, Vol. 23 No. 4, April 2021, P. e21747. DOI:10.2196/21747.

Holmgren, A Jay, Moritz Esdar, Jens Hüsers, João Coutinho-Almeida, "Health Information Exchange: Understanding the Policy Landscape and Future of Data Interoperability", Yearbook of Medical Informatics, Vol. 32 No. 01, August 2023, Pp. 184–194. DOI:10.1055/s-0043-1768719.

Hossain, Md. Khalid, Juliana Sutanto, Putu Wuri Handayani, Anasthasia Agnes Haryanto, Joy Bhowmik, Viviane Frings-Hessami, "An exploratory study of electronic medical record implementation and recordkeeping culture: the case of hospitals in Indonesia", BMC Health Services Research, Vol. 25 No. 1, February 2025, P. 249. DOI:10.1186/s12913-025-12399-0.

Iftikhar, Saman, "Cyberterrorism as a global threat: a review on repercussions and countermeasures", PeerJ. Computer Science, Vol. 10, 2024, P. e1772. DOI:10.7717/peerj-cs.1772.

Keputusan Menteri Kesehatan Republik Indonesia Nomor HK.01.07/MENKES/133/2023 Tentang Integrasi Data Kesehatan Nasional Melalui SATUSEHAT. https://keslan.kemkes.go.id/unduhan/fileunduhan_1689148170_669358.pdf

Khatri, Naresh, "Effective implementation of electronic medical records and health information technologies", Missouri Medicine, Vol. 112 No. 1, 2015, Pp. 41–45.

Lin, Tzu-Wei, Chien-Lung Hsu, Tuan-Vinh Le, Chung-Fu Lu, Bo-Yu Huang, "A Smartcard-Based User-Controlled Single Sign-On for Privacy Preservation in 5G-IoT Telemedicine Systems", Sensors (Basel, Switzerland), Vol. 21 No. 8, April 2021, P. 2880. DOI:10.3390/s21082880.

Nabbilah, Amir, "Legal Protection of Patient Data Confidentiality Electronic Medical Records", Soepra Jurnal Hukum Kesehatan, Vol. 5 No. 2, n.d., Pp. 198–208.

Nguyen, Kim-Huong, Chad Wright, Digby Simpson, Leanna Woods, Tracy Comans, Clair Sullivan, "Economic evaluation and analyses of hospital-based electronic medical records (EMRs): a scoping review of international literature", Npj Digital Medicine, Vol. 5 No. 1, March 2022, P. 29. DOI:10.1038/s41746-022-00565-1.

Novekawati. 2019. Hukum Kesehatan. Semarang: Sai Wawai Publishing.

Ozair, Fouzia F., Nayer Jamshed, Amit Sharma, Praveen Aggarwal, "Ethical issues in electronic health records: A general overview", Perspectives in Clinical Research, Vol. 6 No. 2, 2015, Pp. 73–76. DOI:10.4103/2229-3485.153997.

Passat, Stevanus, Evita Israhadi, "Confidentiality of Medical Record as Legal Protection of Patient's Privacy Rights", Proceedings of the 1st International Conference on Law, Social Science,

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

Economics, and Education, ICLSSEE 2021, March 6th 2021, Jakarta, Indonesia, presented at the Proceedings of the 1st International Conference on Law, Social Science, Economics, and Education, ICLSSEE 2021, March 6th 2021, Jakarta, Indonesia, Salatiga, Indonesia, EAI, 2021. DOI:10.4108/eai.6-3-2021.2306395.

Peraturan Menteri Kesehatan nomor 24 tahun 2022 tentang Rekam Medis. https://peraturan.bpk.go.id/Details/245544/permenkes-no-24-tahun-2022

Peraturan Menteri Kesehatan nomor 36 tahun 2012 tentang Rahasia Kedokteran. https://www.kemhan.go.id/itjen/wp-content/uploads/2017/03/bn915-2012.pdf

Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia nomor 20 tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://peraturan.bpk.go.id/Download/142743/Permen%2520Kominfo%2520Nomor%252020%2520Tahun%25202016.pdf&ved=2ahUKEwinnonU1oSGAxV0wjgGHTyuD9AQFnoECBwQAQ&usg=AOvVaw2Qb4lguMGsngwJGetJ2CjW

Prameswari, Thalia, Wahyu Andrianto, "Pasien: Konsumen Yang Unik", Jurnal Hukum Kesehatan Indonesia, Vol. 1 No. 02, April 2022, Pp. 132–139. DOI:10.53337/jhki.v1i02.8.

Pratiwi, Afiif Hadiani, Edi Wahjuni, Nuzulia Kumala Sari, "Perbuatan Melawan Hukum dalam Kebocoran Data Penumpang Lion Air Group", Journal of Private and Economic Law, Vol. 1 No. 2, n.d., Pp. 107–134.

Putri, Anzany Tania Dwi, "Challenges in implementing electronic medical record in Indonesia healthcare facilities", Jurnal Medika Hutama, Vol. 4 No. 03, n.d., Pp. 3427–31.

Ridwan, Ridwan, "Pertanggungjawaban Hukum Pidana terhadap Pelanggaran Rahasia Medis", Jurnal Hukum & Pembangunan, Vol. 49 No. 2, July 2019, P. 338. DOI:10.21143/jhp.vol49.no2.2007.

Rosidi, Ahamad, M Zainuddin, Ismi Arifiana, "Metode Dalam Penelitian Hukum Normatif Dan Sosiologis (Field Research)", Journal Law and Government, Vol. 2 No. 1, February 2024, P. 46. DOI:10.31764/jlag.v2i1.21606.

Seh, Adil Hussain, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, Raees Ahmad Khan, "Healthcare Data Breaches: Insights and Implications", Healthcare, Vol. 8 No. 2, May 2020, P. 133. DOI:10.3390/healthcare8020133.

Setiawan, Radita, Muhammad Okky Arista, "Efektivitas Undang-Undang Informasi dan Transaksi Elektronik di Indonesia dalam Aspek Hukum Pidana", Recidive, Vol. 2 No. 2, 2013, Pp. 139–146.

Shandler, Ryan, Miguel Alberto Gomez, "The hidden threat of cyber-attacks – undermining public confidence in government", Journal of Information Technology & Politics, Vol. 20 No. 4, October 2023, Pp. 359–374. DOI:10.1080/19331681.2022.2112796.

Sher, Ming-Ling, Paul C. Talley, Ching-Wen Yang, Kuang-Ming Kuo, "Compliance With Electronic Medical Records Privacy Policy: An Empirical Investigation of Hospital Information Technology Staff", INQUIRY: The Journal of Health Care Organization, Provision, and Financing, Vol. 54, January 2017, P. 0046958017711759. DOI:10.1177/0046958017711759.

Sitanggang, Tiromsi. 2019. Aspek Hukum Kepemilikan Rekam Medis Terhadap Perlindungan Hak Pasien. Medan: Penerbit Yayasan Kita Menulis.

Sittig, Dean F., Hardeep Singh, "Rights and responsibilities of users of electronic health records", Canadian Medical Association Journal, Vol. 184 No. 13, September 2012, Pp. 1479–1483. DOI:10.1503/cmaj.111599.

Sonia Dewi, Putu Priyanka, Muharman Lubis, Lukman Abdurrahman, "Aligning Healthcare Strategies Through Digital Information and Technology: Challenges and Solution", 2024

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

12th International Conference on Cyber and IT Service Management (CITSM), 1–6, presented at the 2024 12th International Conference on Cyber and IT Service Management (CITSM), Batam, Indonesia, IEEE, 2024. DOI:10.1109/CITSM64103.2024.10775893.

Sugiarti, Ida, "Legal Protection of Patient Rights to Completeness and Confidentiality in Management of Medical Record Documents", The Proceedings of the 2nd Bakti Tunas Husada-Health Science International Conference (BTH-HSIC 2019), presented at the 2nd Bakti Tunas Husada-Health Science International Conference (BTH-HSIC 2019), Tasikmalaya, Indonesia, Atlantis Press, 2020. DOI:10.2991/ahsr.k.200523.045.

Tilaar, Tirsa Sharon, Pan Lindawaty Suherman Sewu, "Review of Electronic Medical Records in Indonesia and its Developments Based on Legal Regulations in Indonesia and its Harmonization with Electronic Health Records (Manual for Developing Countries)", Daengku: Journal of Humanities and Social Sciences Innovation, Vol. 3 No. 3, April 2023, Pp. 422–430. DOI:10.35877/454RI.daengku1662.

Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. https://peraturan.bpk.go.id/Details/37589/uu-no-11-tahun-2008

Undang-Undang nomor 1 tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023

Undang-Undang nomor 17 tahun 2023 tentang Kesehatan. https://peraturan.bpk.go.id/Details/258028/uu-no-17-tahun-2023

Uslu, Aykut, Jürgen Stausberg, "Value of the Electronic Medical Record for Hospital Care: Update From the Literature", Journal of Medical Internet Research, Vol. 23 No. 12, December 2021, P. e26323. DOI:10.2196/26323.

Wijaya, Yudi Yasmin, Edy Suyanto, Fanny Tanuwijaya, "Rekam Medis: Penggunaan Informasi Medis Pasien dalam Pelaksanaan Asas Perlindungan Publik", Veritas et Justitia, Vol. 6 No. 2, December 2020, Pp. 399–423. DOI:10.25123/vej.3717.

Wijayanti, Dian, Erik Iman Heri Ujianto, Rianto Rianto, "Uncovering Security Vulnerabilities in Electronic Medical Record Systems: A Comprehensive Review of Threats and Recommendations for Enhancement", Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika, Vol. 10 No. 1, February 2024, P. 73. DOI:10.26555/jiteki.v10i1.28192.

Winter, Jenifer Sunrise, Elizabeth Davidson, "Harmonizing regulatory regimes for the governance of patient-generated health data", Telecommunications Policy, Vol. 46 No. 5, June 2022, P. 102285. DOI:10.1016/j.telpol.2021.102285.

Wu, Zongda, Shaolong Xuan, Jian Xie, Chongze Lin, Chenglang Lu, "How to ensure the confidentiality of electronic medical records on the cloud: A technical perspective", Computers in Biology and Medicine, Vol. 147, August 2022, P. 105726. DOI:10.1016/j.compbiomed.2022.105726.

Zlabek, J. A., J. W. Wickus, M. A. Mathiason, "Early cost and safety benefits of an inpatient electronic health record", Journal of the American Medical Informatics Association, Vol. 18 No. 2, March 2011, Pp. 169–172. DOI:10.1136/jamia.2010.007229.