SNLPR:
Siber Nusantara of Law and Politic Review
E-ISSN : 3089-2287
+62 822 1012 3600 https://research.e-siber.org/SNLPR siberpublisher.info@gmail.com

DOI: https://doi.org/10.38035/snlpr.v2i2

LEGAL PROTECTION OF PATIENT MEDICAL RECORDS IN INDONESIA IN REALIZED LEGAL CERTAINTY

Angga Perwira Sukmawinata [1], Prasetyo Edi[2].
[1]Univesitas Borobudur, Jakarta, Indonesia angga.perwira02@gmail.com
[2]Univesitas Borobudur, Jakarta, Indonesia prasmedic@gmail.com

Corresponding Author: prasmedic@gmail.com[1]

Abstract: Medical records are documents containing confidential patient health information and therefore require legal protection. Digitization through electronic medical records has improved the quality of healthcare services, but has also given rise to various legal issues, particularly regarding the protection of patient personal data. Although Indonesia has regulations through Law Number 17 of 2023 concerning Health, Law Number 27 of 2022 concerning Personal Data Protection, Regulation of the Minister of Health Number 24 of 2022 concerning Medical Records, and the Law on Information and Electronic Transactions, these regulations are not yet fully harmonized, thus potentially creating legal uncertainty in the protection of patient medical records. The problems of this research are: (1) how are the regulations for legal protection of patient medical records according to laws and regulations in Indonesia; (2) what form of disharmony exists between the regulations for legal protection of patient medical records between the Health Law, the Law on Personal Data Protection, the Regulation of the Minister of Health on Medical Records, and the Law on Information and Electronic Transactions; and (3) how efforts to harmonize regulations for legal protection of patient medical records can achieve legal certainty in Indonesia. This research is a normative legal study that examines legal norms, legal principles, synchronization of laws and regulations, and legal harmonization through legislative, conceptual, comparative, and analytical approaches. The results of the study indicate that legal protection for patient medical records has been regulated in various laws and regulations. However, there is still disharmony in regulations related to the status of data controllers, patient rights, data protection mechanisms, legal accountability, and the imposition of sanctions, so that they do not fully provide legal certainty. Therefore, regulatory harmonization is needed through synchronization of content between regulations, strengthening personal data protection mechanisms, and affirming the authority and responsibilities of the parties to realize legal certainty in the protection of patient medical records in Indonesia.

Keyword: Legal Protection; Medical Records; Personal Data; Legal Harmonization; Legal Certainty.

Abstrak: Rekam medis merupakan dokumen yang berisi informasi kesehatan pasien yang bersifat rahasia dan oleh karena itu memerlukan perlindungan hukum. Digitalisasi melalui rekam medis elektronik telah meningkatkan kualitas pelayanan kesehatan, namun juga menimbulkan berbagai permasalahan hukum, khususnya terkait perlindungan data pribadi pasien. Meskipun Indonesia telah memiliki regulasi melalui Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis, dan Undang-Undang tentang Informasi dan Transaksi Elektronik, regulasi-regulasi tersebut belum sepenuhnya harmonis, sehingga berpotensi menciptakan ketidakpastian hukum dalam perlindungan rekam medis pasien. Permasalahan dari penelitian ini adalah: (1) bagaimana regulasi perlindungan hukum rekam medis pasien menurut peraturan perundang-undangan di Indonesia; (2) apa bentuk disharmonisasi yang terjadi pada regulasi perlindungan hukum rekam medis pasien antara Undang-Undang Kesehatan, Undang-Undang Perlindungan Data Pribadi, Peraturan Menteri Kesehatan tentang Rekam Medis, dan Undang-Undang Informasi dan Transaksi Elektronik; dan (3) bagaimana upaya harmonisasi regulasi perlindungan hukum rekam medis pasien dapat mencapai kepastian hukum di Indonesia. Penelitian ini merupakan penelitian hukum normatif yang mengkaji norma hukum, asas hukum, sinkronisasi peraturan perundang-undangan, dan harmonisasi hukum melalui pendekatan perundang-undangan, konseptual, komparatif, dan analitis. Hasil penelitian menunjukkan bahwa perlindungan hukum untuk rekam medis pasien telah diatur dalam berbagai peraturan perundang-undangan. Namun, masih terdapat disharmonisasi regulasi terkait status pengendali data, hak pasien, mekanisme perlindungan data, pertanggungjawaban hukum, dan pengenaan sanksi, sehingga belum sepenuhnya memberikan kepastian hukum. Oleh karena itu, harmonisasi regulasi diperlukan melalui sinkronisasi materi muatan antarregulasi, penguatan mekanisme perlindungan data pribadi, serta penegasan wewenang dan tanggung jawab para pihak untuk mewujudkan kepastian hukum dalam perlindungan rekam medis pasien di Indonesia.

Keyword: Payung Hukum; Rekam Medis; Data Pribadi; Harmonisasi Hukum; Kepastian Hukum.

INTRODUCTION

Indonesia, as a nation governed by the rule of law, is strongly committed to providing comprehensive protection for its citizens' rights, one of which is the fundamental right to health. Along with massive technological advancements, the Indonesian healthcare sector is also undergoing a digital transformation that is fundamentally changing the paradigm of patient clinical data management. One concrete form of this digitalization is the use of medical records as crucial documents that capture a patient's entire health history. Medical records are no longer merely technical daily medical records, but have become vital legal documents that serve as valid evidence in court and guarantee the quality of care in healthcare facilities.[1]

Technological acceleration demands the integration of efficient health information systems to improve the speed, accuracy, and efficiency of medical procedures. However, the shift from conventional to electronic systems has created new complexities that challenge the protection of patient personal data. The existence of medical records in the digital ecosystem plays a dualistic role; on the one hand, they are a driving force behind the effectiveness of healthcare services, but on the other, they are highly vulnerable to the risk of privacy violations.

[1]Aris Prio Agus Santoso, *Health Law (Introduction to the Bachelor of Law Study Program)* , Yogyakarta: Pustaka Baru Press, 2022, p. 45.

[2]Therefore, legal protection regulations for medical records need to be strengthened to ensure legal certainty for all parties, including patients as data subjects, healthcare professionals, and hospitals as managers of health information.

Normatively (*das sollen*), the legal framework in Indonesia has actually attempted to compile various regulatory instruments to protect citizens' privacy rights and health data protection. The most fundamental foundation stems from the 1945 Constitution of the Republic of Indonesia, which guarantees the human rights to privacy, self-protection, and the right to adequate health services. This macro policy was then embodied more specifically through the latest sectoral regulations, namely Law Number 17 of 2023 concerning Health, which mandates the digitalization of services while simultaneously protecting patient rights. This protection is strengthened by Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), which expressly categorizes health data as specific personal data that must be protected with high security standards.[3]

At the operational level, the technical aspects of clinical document management are regulated through Minister of Health Regulation Number 24 of 2022 concerning Medical Records, which requires all healthcare facilities in Indonesia to switch to using Electronic Medical Records (EMR). From the perspective of cybersecurity and electronic system reliability, the Law on Information and Electronic Transactions (UU ITE) provides the legal basis for the implementation of electronic systems used in healthcare, including protecting the security of electronic data and information. [4]This series of layered regulations theoretically demonstrates that the state has constructed a solid legal framework to ensure that medical records management is carried out securely, confidentially, and responsibly.[5]

Empirical facts on the ground demonstrate a wide gap between regulatory idealism and the operational reality of healthcare services in Indonesia. The government's accelerated implementation of Electronic Medical Records (EMR) has not been matched by the readiness of technological infrastructure, the reliability of cybersecurity systems, and the equitable digital literacy of human resources across all healthcare facilities. The phenomenon of large-scale health data breaches *affecting* various leading medical institutions is authentic evidence of the fragility of the current healthcare digitalization ecosystem. The threat of increasingly massive and sophisticated cyberattacks, such as ransomware attacks, continues to loom large over hospital data systems, resulting in material and immaterial losses, including a loss of public trust in the confidentiality of their clinical records.[6]

This empirical situation is exacerbated by the tangled threads within the regulatory framework in Indonesia, which has triggered acute disharmony between layers of positive law. Harmonization of regulations between the Health Law, the Personal Data Protection Law (PDP Law), the Minister of Health's Regulation on Medical Records, and the Electronic Information and Transactions Law (ITE Law) has not been optimally realized, resulting in persistent asymmetry in its implementation. On the one hand, the PDP Law imposes very high administrative sanctions and fines on data controllers in the event of protection failures. However, on the other hand, the technical operational governance within the Minister of Health's Regulation on Medical Records has not fully integrated mitigation mechanisms

[2]A. Herisasono, "Legal Protection of Patient Data Privacy in Electronic Medical Record Systems", *Collaborative Journal of Science* , Vol. 7, No. 12, 2024, p. 4678.
[3]Thariq El Saputra, "The Use of Electronic Medical Records in Realizing Legal Protection of Patient Personal Data Security", *Fundamental: Scientific Journal of Law* , Vol. 13, No. 2, 2024, p. 60.
[4]CA Putra & MA Masnun, "Analysis of hospital liability related to potential electronic medical record data leaks due to cybercrime", *Novum: Jurnal Hukum* , Vol. 9, No. 2, 2022, p. 115.
[5]HD Ratman, *Legal Aspects of Informed Consent and Medical Records in Therapeutic Transactions* , Bandung: Keni Media, 2018, p. 72.
[6]A. Herisasono, Op.Cit., p. 4678.

aligned with the personal data protection mandate. [7]This lack of alignment creates a vacuum and overlapping norms that confuse legal practitioners and healthcare industry players in the field.[8]

This legal uncertainty has a direct impact on the blurring of legal liability boundaries among stakeholders. To date, there is no clear and fair formulation of the extent of responsibility for hospitals, healthcare workers as data *inputters* , and third-party *vendors* providing electronic systems in the event of system failures or external data breaches.[5] [9]This weak law enforcement is further emphasized by the lack of an integrated law enforcement mechanism specifically designed to address cybercrime in the medical sector. When patients' privacy rights are violated due to medical record leaks, case resolution is often slow and fails to provide justice and legal certainty for victims.[6][10]

Previous research on medical records has generally focused on conventional and fragmented issues. Most existing academic studies have focused exclusively on maintaining traditional medical confidentiality principles, technical readiness for the adoption of electronic medical records at the management level, or analyzing the Personal Data Protection Law in isolation without linking it to the specifics of medical documents. [11]There is a significant research gap *in* comprehensive inter-regulatory harmonization analysis and the reconstruction of a legal protection model capable of integrating all sectoral laws to achieve integrative legal certainty. This research aims to fill this gap by offering a comprehensive legal review that views law beyond rigid rules and instead reconstructs the regulatory framework to adapt to the dynamics of digital transformation.[12]

The urgency of this research is crucial given its broad implications for human rights protection and the sustainability of the digitalization of the national healthcare sector. Without clear legal reform, patient privacy rights will remain vulnerable, which in turn could undermine public trust in the overall quality of digital healthcare services. [13]Harmonized medical records regulations are essential to ensure strong legal certainty for healthcare facilities and medical personnel, allowing them to innovate without the fear of disproportionate legal sanctions. [14]The results of this research are expected to provide comprehensive, implementable, and problem-solving policy recommendations for policymakers seeking to strengthen legal protection for patient medical records through derivative regulations that can comprehensively protect patient records in Indonesia.

METHODS

This study employed a normative legal research (doctrinal legal research) design to examine the legal framework governing the protection of patient medical records in Indonesia and to analyze the harmonization of regulations aimed at ensuring legal certainty in the digital health sector. The research focused on legal norms rather than empirical observations, emphasizing the consistency, coherence, and interaction of statutory regulations governing medical records, personal data protection, and electronic health systems.

---

[7]SD Rosadi, *Discussion of the Personal Data Protection Law (Law of the Republic of Indonesia No. 27 of 2022)* , Jakarta: Sinar Grafika, 2023, p. 142.
[8]Thariq El Saputra, Op.Cit., p. 63.
[9]Sukardin et al., *Management and Utilization of Health Data: An Epidemiological Perspective* , Sukabumi: Sada Kurnia Pustaka, 2025, p. 54.
[10]RA Prastyanti, *Monograph on the Protection of Consumer Personal Data for Electronic Users* , Pekalongan: Nasya Expanding Management, 2025, p. 88.
[11]Thariq El Saputra, Op.Cit., p. 65.
[12]A. Herisasono, Op.Cit., p. 4679.
[13]SD Rosadi, Op.Cit., p. 145.
[14]CA Putra & MA Masnun, Op.Cit., p. 120.

The study adopted a statutory approach, a conceptual approach, and a comparative regulatory analysis. The statutory approach was used to examine the hierarchy and substance of relevant legislation, including the 1945 Constitution of the Republic of Indonesia, Law Number 17 of 2023 concerning Health, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 11 of 2008 as amended by Law Number 19 of 2016 concerning Electronic Information and Transactions, and Minister of Health Regulation Number 24 of 2022 concerning Medical Records. The conceptual approach was employed to analyze the principles of legal certainty, legal protection, privacy rights, cyber health law, and regulatory harmonization as the theoretical framework for evaluating the coherence of the existing legal system. Comparative regulatory analysis was conducted to identify normative inconsistencies, overlapping authorities, legal gaps, and conflicting regulatory provisions affecting the implementation of legal protection for electronic medical records.

The research relied exclusively on secondary legal materials consisting of primary, secondary, and tertiary legal sources. Primary legal materials included constitutional provisions, statutes, ministerial regulations, and other relevant legislation governing health services, electronic systems, and personal data protection. Secondary legal materials comprised legal doctrines, scholarly books, peer-reviewed journal articles, and previous studies discussing medical records, privacy protection, cybersecurity, and health law. Tertiary legal materials, including legal dictionaries and encyclopedias, were utilized to clarify legal terminology and support conceptual interpretation.

Legal materials were collected through document and literature studies and analyzed using qualitative juridical analysis. The analysis was conducted descriptively and prescriptively by interpreting legal provisions systematically, identifying areas of regulatory disharmony, assessing their implications for legal certainty, and formulating recommendations for regulatory harmonization. The interpretation of legal materials was guided by the principles of statutory interpretation, the doctrine of legal harmonization, and theories of legal certainty, particularly those advanced by Gustav Radbruch and Lon L. Fuller, to evaluate whether the existing regulatory framework adequately guarantees the protection of patients' medical records within Indonesia's digital healthcare system.

RESULTS AND DISCUSSIONS

Current Legal Protection Regulations for Patient Medical Records in Indonesia

Constitutionally, legal protection for medical records is based on the 1945 Constitution of the Republic of Indonesia. Article 28H paragraph (1) guarantees the right to health services, while Article 28G paragraph (1) provides protection for the right to privacy as part of human rights, which is the basis for protecting patient health data and information[1]. Constitutionally, health information is seen as part of human rights for which the state is responsible for providing legal protection.

Legally, medical records are no longer viewed simply as ordinary hospital administrative files. They are defined as documents containing records of a patient's identity, examinations, treatments, medical procedures, and the healthcare services received.[15] This document has a highly strategic dual function: on the one hand, it serves as a clinical instrument for the continuity of medical services, and on the other, it serves as legal evidence that can be used in court proceedings in the event of a medical dispute. [16]Given its content, which includes highly intimate medical histories, medical records are classified as specific personal data that is subject to a higher standard of legal protection than general personal data.[17]

[15]Regulation of the Minister of Health Number 24 of 2022 concerning Medical Records, Article 1 number 1.
[16]HD Ratman, *Legal Aspects of Informed Consent and Medical Records in Therapeutic Transactions* , Bandung: Keni Media, 2018, p. 84.
[17]Thariq El Saputra, Op.Cit., p. 61.

At the sectoral regulatory level, reforms to health law in Indonesia were marked by the enactment of Law Number 17 of 2023 concerning Health. This law reinforces the guarantee of patient confidentiality. This regulation requires healthcare workers and healthcare facilities to maintain the confidentiality of clinical information contained in medical records, both to protect patient rights and to increase public trust in healthcare services.

These regulations are further strengthened by the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which classifies health data as specific personal data. Consequently, any processing of health data must, in principle, be based on the express consent of the patient as the data subject, except in medical emergencies or to comply with statutory provisions. [18]Personal data controllers, in this case healthcare facilities, are required to implement encryption, restrict access, and regular system audits to prevent data leaks.

Along with the development of information technology, the management of medical records is directed towards the use of electronic systems as stipulated in Minister of Health Regulation Number 24 of 2022 concerning Medical Records. This regulation requires all healthcare facilities in Indonesia to implement electronic medical records by the end of 2023. This regulation emphasizes that although the physical documents or electronic systems are owned by healthcare facilities, the contents of the medical records are entirely the property of the patient. [19]Healthcare facilities are fully responsible for accessing, storing, providing network security, and destroying medical records within the specified timeframe.

The security aspect of digital infrastructure is also strengthened through the Electronic Information and Transactions Law (UU ITE). This law prohibits unauthorized access to computers or electronic systems belonging to other parties as a form of protection for the security of electronic information, including hospitals' Electronic Medical Records systems. This cyber regulation closes legal loopholes by imposing serious criminal penalties for those who hack, manipulate data, or illegally intercept patient medical data transmissions flowing within the digital health ecosystem.[20]

From a legal doctrine perspective, legal protection stipulated in Indonesian laws and regulations essentially consists of two forms: preventive legal protection and repressive legal protection. Preventive legal protection is realized through a series of preventative measures before violations occur. Concrete forms include the obligation of healthcare facilities to implement access restrictions (*user access control*), the creation of data security Standard Operating Procedures (SOPs), the implementation of multi-layered encryption systems, and the signing of confidentiality integrity pacts by all medical personnel.[21]

Meanwhile, repressive legal protection functions as a law enforcement instrument that imposes sanctions when a violation or leak of medical record data occurs. This repressive instrument provides three simultaneous avenues of legal accountability. First, the imposition of administrative sanctions in the form of written warnings, administrative fines, and even revocation of the operational permit of a health service facility or a health worker's Practice Permit (SIP). Second, settlement through civil channels by filing a lawsuit based on Unlawful Acts (PMH) to obtain compensation for material and immaterial losses arising from the leak of medical record data. [22]Third, the imposition of criminal sanctions in the form of

[18]SD Rosadi, Op.Cit., p. 165.
[19]Eveline Yulia Darmadi, Imam Ropii, and Nimas Kencana Rukmi, "Legal Protection *of Electronic Medical Records in Dental Practice* ", *Journal of Health Law and Ethics* , Vol. 6, No. 1, 2025, p. 38.
[20]RA Prastyanti, Op.Cit., p. 102.
[21]Rospita Adelina Siregar, "Implementation of Minister of Health Regulation Number 24 of 2022 concerning Medical Records on the Effectiveness of Health Services", *Kyadiren Journal of Legal Studies* , Vol. 5, No. 2, 2024, p. 7.
[22]CA Putra & MA Masnun, Op.Cit., p. 118.

imprisonment and fines against anyone proven to have unlawfully leaked, traded, or accessed patient medical record documents without authorization.

Disharmony in the Regulations on Legal Protection of Patient Medical Records Between the Health Law, the Personal Data Protection Law, the Minister of Health Regulation on Medical Records, and the Electronic Information and Transactions Law

The disharmony in the legal protection of patient medical records between the Health Law, the Personal Data Protection Law (PDP Law), Minister of Health Regulation No. 24 of 2022, and Law No. 11 of 2008 in conjunction with Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE) is not a direct conflict between these norms, but rather a lack of synchronization in regulations, overlapping authority, a lack of norms, and differences in legal regimes. This disharmony can be explained as follows.

First, there is a lack of clarity regarding the legal standing between data controllers and data processors. The PDP Law regulates both concepts and their legal responsibilities, but their implementation in the healthcare sector remains unclear. [23]In contrast, Minister of Health Regulation No. 24 of 2022 only uses traditional nomenclature such as Health Service Facilities (Fasyankes), Medical Records Providers, and Healthcare Workers. [24]This lack of synchronization of terms creates a legal vacuum (*rechtshacuüm*) regarding whether hospitals automatically act as Personal Data Controllers or merely technical processors. This ambiguity makes it difficult to determine who is legally responsible in the event of a patient's medical data breach.

Second, the asymmetry in the regulation of patient rights over clinical documents. The PDP Law provides data subjects with very broad digital rights, including the right to obtain information, the right to access data, the right to correct data, the right to withdraw consent, and *the right to erase data* . In contrast, Minister of Health Regulation Number 24 of 2022 restricts ownership by stating that the contents of medical records belong to the patient, but the physical files or electronic systems belong to the healthcare facility. [25]The Minister of Health Regulation has not yet formulated in detail the mechanisms for patients to request complete copies, the right to correction, the right to object, or the right to erase their medical data. Yet, these rights are mandatory instruments fully recognized under the PDP Law.

Third, the divergence of consent mechanisms *in* medical procedures and data processing. The PDP Law stipulates that personal data processing can only be carried out if there is a lawful basis *,* including explicit consent given by the data subject. [26]In contrast, in the healthcare ecosystem, patient clinical data can be processed automatically for emergencies or medical services without the rigid *consent mechanisms mandated by the PDP Law. Furthermore, Minister of Health Regulation No. 24 of 2022 does not provide rigid guidelines* regarding when healthcare facilities are required to request new consent from patients when their medical data is used for secondary purposes outside of services, such as research, education, or global health analysis.

Fourth, the lack of synchronized procedures for reporting data breaches. The Personal Data Protection Law requires every Personal Data Controller to report incidents of data protection failures to the data subject and authorized institutions. [27]However, Minister of Health Regulation No. 24 of 2022 lacks a legal framework because it does not specifically

[23]Law Number 27 of 2022 concerning Personal Data Protection, Article 1 number 4, Article 1 number 5, and Articles 20 to 39

[24]Minister of Health Regulation Number 24 of 2022 concerning Medical Records, Article 3 – Article 11.

[25]Riezky Danang Dady, “Legal Protection of Patient Personal Data in Electronic Medical Records”, *Glosains: Indonesian Global Science Journal* , Vol. 7, No. 2, 2026, p. 675.

[26]CA Putra & MA Masnun, Op.Cit., p. 116.

[27]Law Number 27 of 2022 concerning Personal Data Protection, Article 46.

regulate the time limit for reporting breaches, the format for formal notification to patients, procedures for mitigating victim recovery, or a compensation scheme for data breaches. This lack of uniform sectoral guidelines leaves hospital management at a loss and lacking definitive operational standards when facing cyberattacks or data breaches.

Fifth, overlapping sanctions regimes and electronic system integration. Disharmonious enforcement of sanctions has created acute uncertainty due to the operation of three distinct regimes without clear legal interconnections. The PDP Law threatens violators with administrative sanctions, civil damages, and corporate criminal sanctions. Meanwhile, the ITE Law focuses criminal sanctions on hacking (*illegal access*), illegal interception, and cyber data manipulation. [28]Meanwhile, Minister of Health Regulation No. 24 of 2022 only emphasizes internal administrative sanctions against healthcare facilities.

As a result, legal enforcement is unclear: whether medical record hacking is prosecuted under the ITE Law, hospital negligence under the PDP Law, or health worker leaks under the Health Law. This situation is exacerbated by the obligation of healthcare facilities to interoperate with the Ministry of Health's SATUSEHAT platform. Existing regulations do not yet provide clarity regarding the division of legal responsibility between healthcare facilities, the Ministry of Health, and the Hospital Management Information System (SIMRS) vendor. When leaks occur during data exchange (*data in transit*) between systems, this lack of clarity creates the risk of overlapping liability *,* making it difficult to determine the guilty party.

Based on the discussion above, the root of the main problem in protecting medical records in Indonesia is not caused by a legal vacuum resulting from a lack of regulations. Indonesia already has a very dense, comprehensive, and multi-layered regulation. However, the fundamental weakness stems from the lack of integration between national laws and regulations due to the formation of ego-sectoral laws. This has resulted in overlapping and contradictory regulations, thus crippling the value of legal certainty. Therefore, material reconciliation through harmonization of laws and regulations is a legal imperative to ensure the realization of solid legal certainty and the protection of patient rights in the era of digital health transformation.

Harmonization of Legal Protection Regulations for Patient Medical Records to Achieve Legal Certainty in Indonesia

According to the theory of legislation, the formation of legislation must be guided by the principle of conformity between types, hierarchies, and content materials, and must reflect inner harmony both vertically and horizontally to prevent the occurrence of norm conflicts (*norm conflict*). [29]The arrangement of clinical data protection in the digital ecosystem must not be born partially by each ministry or sectoral institution, but must be constructed as a unified system of norms that are complete, logical, and hierarchical in accordance with the order of national legislation.[30]

The need for integration of this content material is directly proportional to the fulfillment of Gustav Radbruch's theory of legal certainty. Radbruch outlined that legal certainty (*Rechtssicherheit*) is the main pillar that demands that positive law be formulated clearly (*clarity*), normatively consistent (*consistency*), and objectively predictable by legal subjects (*predictability*). [31]Lon Fuller complements this view by stating that acute uncertainty arises when there are internal contradictions within the legal rules themselves (*contradictions in*

[28]Law Number 27 of 2022 concerning Personal Data Protection, Article 30, Article 31, Article 32, and Article 35.
[29]Maria Farida Indrati S., *Legal Science: Types, Functions, and Content Material* , Yogyakarta: Kanisius, 2020, p. 94.
[30]Ibid., p. 102.
[31]Bernard L. Tanya, *Radbruch's Legal Theory in the Dynamics of Legal Certainty* , Jakarta: Rajawali Press, 2021, p. 57.

legislation). [32]When medical record regulations in Indonesia are trapped in a dualism of interpretation between privacy protection and mandatory administrative fulfillment, healthcare facilities will lose operational predictability of action and patients lose the guarantee of protection of their privacy rights in essence.

The first tactical step to uphold the value of legal certainty is to harmonize the content of laws and regulations horizontally. The actual implementation of this synchronization model aims to integratively align the content of the Health Law, the PDP Law, the Minister of Health Regulation on Medical Records, and the ITE Law. This alignment of legal material is urgently needed to eliminate overlapping *law* enforcement authorities and fill the legal vacuum (*rechtshacuüm*) that triggers doubts among medical practitioners in the field.[33]

Through this adjustment of the content, the differences in regulations contained in sectoral laws and regulations can be harmonized through the application of the principle of *lex specialis derogat legi generali* in accordance with the characteristics of each regulation. This philosophical alignment aims to bridge the gap between the human right to guaranteed health services and individual sovereignty over the protection of the privacy of their digital personal data. [34]This affirmation of the legal material ensures that the disclosure of health data for the public interest does not compromise fundamental patient protection standards. This arrangement of the material also serves as the initial foundation for constructing a consistent and coherent legal framework under the corridor of the principle of legality in the formation of valid laws.

Second, strengthening the protection of Electronic Medical Records (EMR). The new legal framework must provide absolute legal confirmation of the legal status of medical records as sensitive personal data *,* in accordance with the national cyber mandate. This specific classification carries legal consequences, requiring the processing of digital patient clinical files to be subject to higher-level technological protection standards that are far more stringent than those for general personal data. [35]This affirmation of the specific data status serves as a primary legal shield, protecting patients from the threat of illegal commercialization of health information on digital networks.

In line with strengthening the protection of EMRs, implementing regulations must clearly define the legal boundaries between the positions of Data Controllers *and* Data Processors *in* the healthcare sector. Legal regulations must stipulate that healthcare facilities bear the highest accountability as data controllers responsible for the security of clinical document storage. [36]On the other hand, third-party vendors providing Hospital Management Information Systems (SIMRS) software are positioned as data processors and are required to comply with the controller's instructions. [37]This regulation is complemented by mandatory standardization regarding information security and EMR cybersecurity, including the implementation of *user access control* through a strict dual authentication system.

Third, equitable legal harmonization must prioritize human interests by strengthening patient rights and protection. The resulting synchronized regulations must affirm patients' rights to access, correct, and obtain complete transparency regarding the use of their medical records. This right to digital access must no longer be hampered by healthcare facility

[32]Ibid., p. 63.
[33]I. Indra, TN Dewi, and DB Wibowo, "Protection of Patient Data Confidentiality vs. the Obligation to Open Access to Electronic Medical Records", *Soepra Journal of Health Law* , Vol. 10, No. 1, 2024, p. 104.
[34]N. Juwita, "Legal Analysis of Electronic Medical Record Regulations Following the Enactment of the Personal Data Protection Law", *Transnational Law Journal* , Vol. 11, No. 2, 2025, p. 45.
[35]Nur Afifah, et al., "Analysis of Information Security Aspects of Patient Data in Electronic Medical Records", *Indonesian Journal of Health Information Management* , Vol. 13, No. 1, 2025, p. 75.
[36]Gunawan Widjaja, "Legal Protection for Patients and Medical Personnel in Digital Health Innovation", *Jurnal Kesehatan* , Vol. 3, No. 2, 2025, p. 18.
[37]N. Juwita, Op.Cit., p. 49.

bureaucracy under the pretext that ownership of electronic system files is under the unilateral control of hospital management. [38]Patients have the right to periodically know the digital audit trail *of* any external parties who have disclosed their personal medical records.

Furthermore, digital health governance must adopt rigid *consent mechanisms* and restrict access to medical records in a multi-layered manner. Patients must be granted legal sovereignty in the form of the right to explicit consent *regarding* the use of their medical data for secondary purposes beyond treatment, such as academic research or pharmaceutical industry commercialization. [39]To anticipate system failures, regulations must establish mandatory procedures for immediate reporting of data breach *notification* . Healthcare facilities are burdened with strict deadlines to formally report cyber incidents to data subjects and supervisory authorities to minimize the risk of social harm to victims.[40]

Fourth, the final manifestation of legal certainty boils down to strengthening accountability and law enforcement mechanisms. Integrated regulations must include a proportional affirmation of responsibility between hospitals, healthcare workers as data inputters, electronic system providers (*vendors*), and third parties who utilize health data. Hospitals are burdened with corporate liability *for* negligence in internal security systems, while vendors are responsible for hidden product defects in the SIMRS application. [41]This transparent definition of responsibility eliminates the culture of assigning jurisdictional blame in the event of a cyberattack or data breach.

This law enforcement measure is enhanced by harmonizing administrative, civil, and criminal sanctions across sectoral laws. Graduation of penalties must be formulated proportionally to ensure that administrative sanctions imposed do not cripple the humanitarian service function of regional public hospitals. [42]Criminal sanctions in the PDP Law and the ITE Law must be harmoniously combined to ensnare perpetrators of medical cybercrime (*cyber-attackers*), while civil sanctions provide a pathway for patients to seek fair compensation. [43]Strengthening oversight mechanisms through a single integrated supervisory authority is key to ensuring legal compliance for digital health institutions.

An integrated regulatory model for legal certainty involves the development of implementing regulations or integrated cross-sectoral guidelines to address current legal fragmentation. This model is realized by formulating a single derivative Government Regulation that cohesively integrates provisions in the Health Law, the PDP Law, the Minister of Health's Regulation on Medical Records, and the ITE Law. This regulatory bridge strengthens formal coordination channels between the Ministry of Health, the personal data protection supervisory authority, healthcare organizations, and electronic system providers. This integrative model ensures that all cyber-medical actors operate within a unified, legitimate and controlled operational framework.

From the discussion above, regulatory harmonization is a strategic step towards building an integrated legal protection system for medical records. Regulatory harmonization ensures that public health data is managed securely, confidentially, and accountably based on solid positive law. Clarity about the rights and obligations of all parties can eliminate legal concerns, strengthen legal accountability mechanisms, and realize the essential value of legal certainty in the management of patient medical records in Indonesia. This regulatory arrangement is an

[38]R. Rayyan and ARM Siregar, "Legal Certainty in the Implementation of Health Technology: Patient Data Protection and Malpractice", *Politika Progresif: Journal of Law, Politics and Humanities* , Vol. 2, No. 1, 2025, p. 82.
[39]I. Indra, TN Dewi, and DB Wibowo, Op.Cit., p. 110.
[40]Nur Afifah, et al., Op.Cit., p. 77.
[41]Gunawan Widjaja, Op.Cit., p. 22.
[42]R. Rayyan and ARM Siregar, Op.Cit., p. 88.
[43]Maria Farida Indrati S., Op.Cit., p. 115.

absolute prerequisite for building public trust *and* protecting the nation's health data sovereignty in the era of digital transformation.

CONCLUSION

The regulation of medical records in Indonesia has been normatively established through a layered and hierarchical legal framework, beginning with the 1945 Constitution of the Republic of Indonesia, Law Number 17 of 2023 concerning Health, Law Number 27 of 2022 concerning Personal Data Protection, the Electronic Information and Transactions Law, and the Regulation of the Minister of Health Number 24 of 2022 concerning Medical Records. Collectively, these legal instruments recognize medical records as specific personal data that must be protected through preventive and repressive legal mechanisms. Nevertheless, despite the existence of this comprehensive legal framework, regulatory disharmony persists due to sectoral and overlapping arrangements that create legal uncertainty. This disharmony is reflected in the unclear legal relationship between health facilities as Data Controllers, the asymmetry in protecting patients' digital rights, particularly the right to erasure, differences in the legal basis for obtaining patient consent, the absence of standardized procedures for reporting and handling personal data breach incidents, and overlapping sanction regimes arising from the interoperability of health information systems, including the SATUSEHAT platform. Therefore, achieving genuine legal certainty requires comprehensive cross-sectoral regulatory harmonization through the formulation of a Government Regulation derived from the Personal Data Protection Law specifically for the health sector. Such regulation should integrate the principles of cyber health law, harmonize legal terminology, standardize explicit patient consent mechanisms within the SATUSEHAT ecosystem, establish a unified national reporting system for personal data breach incidents, clarify the distribution of legal responsibility between health facilities and third-party vendors, and strengthen the protection of patients' digital rights in order to restore public trust in Indonesia's digital health system. Furthermore, health facilities and hospitals should proactively conduct independent cybersecurity audits, strengthen Standard Operating Procedures (SOPs) governing user access control, implement layered encryption technologies, and ensure that cooperation agreements with third-party Hospital Management Information System (SIMRS) vendors include strict liability clauses for personal data protection. Finally, the House of Representatives and the Government should revise or clarify the provisions concerning the retention period of medical records under the Minister of Health Regulation on Medical Records to ensure consistency with the data deletion principle embodied in the Personal Data Protection Law, thereby preventing future normative conflicts and strengthening the effectiveness of cyber health law enforcement in Indonesia.

REFERENSI

Dady, Riezky Danang. *" Legal Protection of Personal Data" Patient on Record Electronic Medicine ."* Glosains : Indonesian Global Science Journal , Vol. 7, No. 2, 2026.

Darmadi, Eveline Yulia, Imam Ropii , and Nimas Kencana Rukmi. *" Legal Protection of Records Electronic Medical in Practice Dentistry : Legal Protection of Electronic Medical Records in Dental Practice."* Journal of Health Law and Ethics, Vol. 6, No. 1, 2025.

Herisasono , A. *" Legal Protection for Patient Data Privacy in System Record Electronic Medical* Journal Collaborative Science, Vol. 7, No. 12, 2024.

Indra, I., TN Dewi, and DB Wibowo. *" Protection Patient Data Confidentiality vs. Obligations Open Record Access Electronic Medical ."* Soepra Journal of Health Law, Vol. 10, No. 1, 2024.

Juwita, N. *" Analysis Juridical Arrangement Record Electronic Medicine After the Enactment of the Personal Data Protection Law ."* Journal of Transnational Law , Vol. 11, No. 2, 2025.

Putra, CA, and MA Masnun . *" Analysis Responsibility of Related Hospitals Potential Record Data Leak Electronic Medical Devices Due to Cyber Crime."* Novum: Jurnal Hukum, Vol. 9, No. 2, 2022.

Rayyan, R., and ARM Siregar. *" Legal Certainty in Implementation Health Technology : Patient Data Protection and Malpractice ."* Progressive Politics : Journal of Law, Politics and Humanities , Vol. 2, No. 1, 2025.

Saputra, Thariq El. *" Use of Electronic Medical Records in Realize Legal Protection of Personal Data Security Patients ."* Fundamentals: Journal Scientific Law, Vol. 13, No. 2, 2024.

Siregar, Rospita Adelina. " *Implementation Minister of Health Regulation Number 24 of 2022 Concerning Record Medical To Effectiveness Health Services ."* Journal Kyadiren Legal Studies , Vol. 5, No. 2, 2024.

Widjaja, Gunawan. *" Legal Protection for Patients and Medical Personnel" in Digital Health Innovation ."* Journal of Health, Vol. 3, No. 2, 2025.

Nur Afifah, et al . *" Analysis of Security Aspects Patient Data Information on Records Electronic Medical"* Journal Management Indonesian Health Information , Vol. 13, No. 1, 2025.