Legal Reconstruction of Electronic Health Data Protection in Indonesia's Digital Health Ecosystem

Dhian Indah Astanti[1], Anggraeni Endah Kusumaningrum[2]

[1]Doctoral Program in Law, Universitas 17 Agustus 1945 Semarang, Semarang, Indonesia, dhian.indah@usm.ac.id

[2]Department of Health Law, Universitas 17 Agustus 1945 Semarang, Indonesia, anggraeni@untagsmg.ac.id

Corresponding Author: dhian.indah@usm.ac.id

Abstract

The rapid expansion of Indonesia's digital health ecosystem has heightened the urgency for strong legal protection of electronic health data. Existing frameworks, including the 1945 Constitution, Law No. 27/2022 on Personal Data Protection, Law No. 17/2023 on Health, Government Regulation No. 71/2019, and Minister of Health Regulation No. 24/2022, remain weakened by regulatory inconsistency, fragmented governance, limited institutional coordination, and insufficient regulation of emerging technologies. This study employs normative juridical research with statutory, conceptual, and comparative approaches, supported by qualitative prescriptive analysis. Comparative references to the EU's GDPR and the US HIPAA highlight internationally recognized standards. Findings indicate that incremental amendments are inadequate, and comprehensive legal reconstruction is required. To address this, the Five-Pillar Legal Protection Model is proposed: Legal Substance Reform, Institutional Governance, Cybersecurity Integration, Patients' Rights Protection, and Oversight and Law Enforcement. This model advances legal protection scholarship by transforming conventional frameworks into an integrated governance system that enhances legal certainty, institutional accountability, cybersecurity resilience, and patient rights within Indonesia's digital health ecosystem.

Keywords: *Electronic Health Data; Digital Health Governance; Legal Protection; Patients' Rights; Five-Pillar Legal Protection Model.*

A. INTRODUCTION

The rapid digital transformation of healthcare has fundamentally changed the management and delivery of health services worldwide. The integration of electronic medical records, telemedicine, artificial intelligence (AI), wearable health devices, cloud computing, and interoperable health information systems has improved healthcare efficiency, expanded access to medical services, and

enhanced evidence-based clinical decision-making (Salami, 2022). At the same time, these technological developments have significantly increased the volume, complexity, and strategic value of electronic health data.

Unlike ordinary personal information, electronic health data contain highly sensitive information relating to an individual's physical and mental condition, medical history, genetic characteristics, diagnosis, and treatment records (Shabani & Yilmaz, 2022). Consequently, inadequate legal protection may expose patients to privacy violations, discrimination, identity theft, unauthorized commercial exploitation, and cyberattacks that threaten both individual rights and public trust in digital healthcare systems.

Indonesia has accelerated digital health transformation through the implementation of the SATUSEHAT Indonesia Platform, mandatory electronic medical records under Law Number 17 of 2023 concerning Health, and broader integration of digital health services within the national healthcare system (Salami, 2024). These initiatives demonstrate the Government's commitment to improving healthcare quality through digital innovation while promoting interoperability among healthcare providers.

Nevertheless, the increasing interconnection of health information systems has simultaneously generated more complex legal challenges, including unauthorized access to medical records, secondary use of health data without valid consent, cross-border data transfers, algorithmic decision-making using artificial intelligence, and cybersecurity threats targeting healthcare infrastructure (Benseghir, Zerara, et al., 2025). These developments indicate that legal protection of electronic health data can no longer be understood solely as an issue

of personal data privacy but must also encompass governance, institutional accountability, technological security, and the protection of patients' constitutional rights.

Indonesia has established several legal instruments governing electronic health data protection, including the 1945 Constitution of the Republic of Indonesia, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 17 of 2023 concerning Health, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and Minister of Health Regulation Number 24 of 2022 concerning Medical Records (Benseghir, Bentria, Zerara, & Bendriss, 2025). Collectively, these regulations provide an important legal foundation for protecting personal data and regulating digital healthcare services. However, because these legal instruments originate from different regulatory sectors and were enacted for different policy objectives, they operate as separate legal regimes rather than as a unified legal framework specifically designed to govern electronic health data (De Anna, 2022). This condition has resulted in fragmented regulation, overlapping institutional authority, inconsistent cybersecurity obligations, and legal uncertainty regarding emerging digital technologies.

The legal challenges associated with electronic health data have attracted increasing scholarly attention. Previous studies have made valuable contributions by examining various dimensions of digital health regulation, yet most have concentrated on specific legal issues rather than developing an integrated legal protection framework. Hendra et al. (2022) analyzed personal data protection in Indonesian electronic health services and identified several regulatory weaknesses

affecting privacy protection. Nevertheless, their study primarily focused on the implementation of existing legislation without proposing a comprehensive legal reconstruction model capable of integrating regulatory reform, institutional governance, and technological safeguards. Similarly, Jain (2023) discussed legal and ethical challenges associated with digital healthcare governance in India, emphasizing regulatory adaptation to artificial intelligence and technological innovation.

Although offering valuable comparative insights, the study remained limited to governance issues within the Indian legal system and did not formulate a broader normative framework applicable to Indonesia. Meanwhile, Lestari et al. (2024) examined electronic health records from legal and technological perspectives, focusing mainly on operational information security and electronic medical record management without comprehensively addressing legal harmonization, institutional coordination, patients' rights, and oversight mechanisms within Indonesia's evolving digital health ecosystem.

The limitations of previous studies reveal three interconnected research gaps. The first is a practical gap, namely the continued existence of regulatory fragmentation and institutional overlap that weaken the effectiveness of electronic health data governance despite the availability of multiple legal instruments (Fauziah et al., 2025). The second is a normative gap, reflected in the absence of an integrated legal framework capable of governing emerging issues such as artificial intelligence in healthcare, health data interoperability, cloud-based medical information systems, genomic data, secondary use of health information, and cross-border electronic health data transfers. The third is a theoretical gap.

Existing legal scholarship generally employs legal protection theory, privacy theory, or digital health governance theory independently. However, no previous study has reconstructed these theoretical perspectives into a unified legal protection model capable of integrating legal substance, institutional governance, cybersecurity, patients' rights, and oversight mechanisms within a single normative framework specifically designed for Indonesia's digital health ecosystem (Sekalala et al., 2026).

The existence of this theoretical gap demonstrates that the principal challenge is not merely the absence of legislation but the absence of a coherent legal theory capable of explaining how legal protection should operate within a rapidly evolving digital health environment (van Kolfschooten et al., 2026). Philipus M. Hadjon's theory of legal protection distinguishes preventive and repressive legal protection as the primary mechanisms for safeguarding individual rights (Chan, 2026).

Likewise, Lawrence Friedman's Legal System Theory explains legal effectiveness through the interaction of legal substance, legal structure, and legal culture. Although these theories remain highly influential, neither was originally developed to address the governance complexities arising from electronic health data processing, artificial intelligence, cybersecurity, interoperability, or transnational digital health ecosystems (Mardiansyah et al., 2025). Consequently, the existing theoretical framework requires further development to remain responsive to contemporary digital governance challenges.

Accordingly, this study does not merely recommend regulatory harmonization but proposes a Five-Pillar Legal Protection Model as a normative

reconstruction of legal protection theory within the context of digital health governance (Benseghir, Bentria, Zerara, Bendriss, et al., 2025). The proposed model expands classical legal protection theory by transforming legal protection from a reactive mechanism responding to legal violations into a continuous governance framework operating throughout the entire lifecycle of electronic health data.

Simultaneously, the model develops Friedman's Legal System Theory by extending its traditional components of legal substance and legal structure through the incorporation of cybersecurity integration, patients' rights protection, and integrated oversight as autonomous normative pillars required for governing sensitive electronic health information. Therefore, the Five-Pillar Legal Protection Model should be understood not merely as a policy recommendation but as a theoretical development contributing to contemporary legal scholarship concerning digital health governance.

Based on these considerations, this study addresses two research questions. First, how is electronic health data currently regulated within Indonesia's digital health ecosystem? Second, how should Indonesia reconstruct its legal protection framework to ensure legal certainty, data security, institutional accountability, and effective protection of patients' rights amid continuing digital health transformation? By answering these questions, this research seeks to contribute not only to the reform of Indonesian health law but also to the development of legal protection theory through an integrated normative model capable of guiding future regulation of electronic health data in the digital era.

B. RESEARCH METHOD

This study employs normative juridical legal research, which conceptualizes law as a system of norms comprising constitutional provisions, statutory regulations, legal principles, legal doctrines, judicial reasoning, and scholarly opinions that are systematically examined to formulate legal arguments and legal reconstruction (Wulandari, 2025). The research focuses on evaluating the legal framework governing electronic health data protection in Indonesia and reconstructing an integrated legal protection model capable of ensuring legal certainty, cybersecurity, institutional accountability, and the protection of patients' rights within the digital health ecosystem.

To achieve these objectives, the study adopts three complementary approaches: the statutory approach, the conceptual approach, and the comparative approach (Muhaimin, 2023). The statutory approach examines the hierarchy, consistency, and interaction among the principal legal instruments governing electronic health data protection, including the 1945 Constitution of the Republic of Indonesia, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 17 of 2023 concerning Health, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and Minister of Health Regulation Number 24 of 2022 concerning Medical Records. These legal instruments are analyzed to identify regulatory inconsistencies, normative fragmentation, overlapping institutional authority, and legal gaps concerning emerging digital health technologies.

The conceptual approach provides the theoretical foundation for evaluating the adequacy of Indonesia's legal framework. This study employs Philipus M.

Hadjon's theory of legal protection, Lawrence Friedman's Legal System Theory, Hans Kelsen's theory of normative hierarchy, and Ronald Dworkin's theory of law as integrity. These theories are used as analytical benchmarks to assess whether the existing legal framework provides coherent and effective protection for electronic health data while also serving as the normative basis for reconstructing a more integrated legal protection model. Rather than merely describing legal norms, the conceptual analysis evaluates their consistency with the principles of legal certainty, justice, legal protection, and good governance in the context of digital healthcare.

The comparative approach applies functional comparative legal analysis by examining Indonesia's legal framework alongside the European Union's General Data Protection Regulation (GDPR) and the United States Health Insurance Portability and Accountability Act (HIPAA). These two regulatory regimes were selected because they represent internationally recognized standards for protecting electronic health data through different regulatory approaches. The GDPR establishes a comprehensive human rights-based personal data protection regime applicable across sectors, whereas HIPAA provides a sector-specific framework dedicated exclusively to healthcare information. The comparison is intended to identify similarities, differences, and best practices that may contribute to strengthening Indonesia's legal framework, particularly regarding institutional governance, cybersecurity standards, patients' rights, breach notification mechanisms, and cross-border health data transfers.

The legal materials consist of primary, secondary, and tertiary legal materials collected through library research (Smits, 2021). Primary legal materials

include constitutions, statutes, government regulations, ministerial regulations, and international legal instruments governing personal data protection and digital health. Secondary legal materials comprise peer-reviewed journal articles, scholarly books, legal commentaries, and academic publications discussing legal protection, digital health governance, privacy, cybersecurity, and comparative health law. Tertiary legal materials include legal dictionaries, encyclopedias, and other reference materials used to clarify legal concepts and terminology. All legal materials were selected based on their authority, relevance, and contribution to the research objectives.

The collected legal materials were analyzed qualitatively using prescriptive legal analysis supported by grammatical, systematic, teleological, and comparative interpretation (Van Hoecke, 2018). Grammatical interpretation was employed to determine the ordinary meaning of statutory provisions governing electronic health data protection. Systematic interpretation examined the relationship among constitutional provisions, personal data protection legislation, health law, and electronic system regulations to evaluate normative consistency and regulatory coherence. Teleological interpretation was applied to identify the legislative objectives underlying privacy protection, healthcare governance, and patients' rights, while comparative interpretation evaluated Indonesia's regulatory framework against internationally recognized legal standards. These complementary methods enabled the identification of normative deficiencies requiring legal reconstruction.

The analytical process was conducted sequentially (Hutchinson & Duncan, 2017). The research first identified and evaluated the existing legal framework

governing electronic health data protection in Indonesia to determine its consistency, coherence, and effectiveness in responding to digital health governance. The findings of the normative evaluation were subsequently examined using the theoretical perspectives adopted in this study and were further strengthened through comparative analysis with the GDPR and HIPAA. The synthesis of the normative and comparative analyses was then used to formulate a prescriptive legal reconstruction that addresses the regulatory fragmentation, institutional overlap, and governance gaps identified throughout the study. This analytical process ultimately produced the Five-Pillar Legal Protection Model as an integrated normative framework intended to strengthen electronic health data protection in Indonesia while contributing to the development of legal scholarship concerning digital health governance.

C. RESULT AND DISCUSSION

1. Normative Evaluation and Comparative Analysis of Electronic Health Data Protection in Indonesia's Digital Health Ecosystem

Indonesia's digital health transformation has significantly increased the collection, processing, storage, and exchange of electronic health data through electronic medical records, telemedicine, and the SATUSEHAT Indonesia Platform. Technological innovation has improved healthcare efficiency, interoperability, and service accessibility. Nevertheless, rapid digitalization has also generated complex legal issues concerning privacy, cybersecurity, institutional accountability, and patients' rights (Akkhateerathitiphum, 2026). Effective legal protection therefore requires

not only comprehensive legislation but also a coherent regulatory system capable of governing the entire lifecycle of electronic health information.

The constitutional foundation for electronic health data protection originates from Articles 28G paragraph (1) and 28H paragraph (1) of the 1945 Constitution of the Republic of Indonesia. Article 28G guarantees personal security, dignity, honour, and privacy, whereas Article 28H recognizes every person's right to obtain healthcare services (Putri, 2026). These constitutional guarantees establish electronic health data as highly sensitive personal information requiring a higher level of legal protection than ordinary personal data because unauthorized disclosure may adversely affect individual rights, healthcare access, and public confidence in digital health services.

Indonesia has established a legal basis through Law Number 27 of 2022 concerning Personal Data Protection, Law Number 17 of 2023 concerning Health, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and Minister of Health Regulation Number 24 of 2022 concerning Medical Records (Jawed & Girish, 2026). Collectively, these legal instruments regulate personal data protection, healthcare administration, electronic systems, and medical records. However, each regulation serves a different legislative objective and operates under separate regulatory sectors. Such conditions prevent the formation of an integrated governance framework specifically designed for electronic health data protection.

Normative analysis demonstrates that the principal weakness of the existing legal framework arises from regulatory inconsistency rather than

legislative absence. The Personal Data Protection Law establishes general principles governing personal data processing but provides no specific provisions governing artificial intelligence-assisted diagnosis, health data interoperability, genomic information, secondary use of medical data, cloud-based medical records, or international transfers of electronic health information (Smit et al., 2024). The Health Law promotes digital healthcare transformation but contains limited provisions concerning institutional coordination, cybersecurity governance, and supervisory mechanisms. Government Regulation Number 71 of 2019 regulates electronic systems generally, whereas Minister of Health Regulation Number 24 of 2022 concentrates primarily on electronic medical records. Consequently, electronic health data governance remains dispersed across several legal instruments without a unified regulatory architecture.

Hans Kelsen's theory of normative hierarchy provides an appropriate analytical basis for evaluating regulatory coherence. Every lower legal norm should consistently implement higher legal norms without creating contradiction or ambiguity (Kusuma et al., 2022). Examination of Indonesia's regulatory structure demonstrates that constitutional guarantees relating to privacy and healthcare have not yet been translated into a coherent system governing electronic health data. Lawrence Friedman's Legal System Theory further explains that legal effectiveness depends upon the harmonious interaction between legal substance and legal structure. Indonesia possesses adequate statutory instruments, yet institutional coordination remains fragmented, reducing regulatory effectiveness and legal certainty.

Normative evaluation also identifies several governance deficiencies associated with technological development. Existing legislation provides only limited guidance concerning artificial intelligence, machine-learning applications for clinical decision-making, cloud-based medical information systems, secondary use of electronic health data, genomic information, and international transfers of health information (Greenhalgh et al., 2020). Rapid technological advancement has therefore exceeded the adaptive capacity of existing legislation, creating governance gaps that may compromise legal certainty and effective protection of patients' rights.

Philipus M. Hadjon's theory of legal protection distinguishes preventive legal protection from repressive legal protection. Examination of Indonesia's current legal framework indicates greater emphasis on repressive mechanisms through administrative sanctions and legal liability following personal data breaches. Preventive mechanisms remain relatively limited because existing legislation does not comprehensively regulate mandatory healthcare cybersecurity standards, sector-specific risk management, interoperability governance, or integrated supervisory mechanisms. Such conditions indicate that legal protection continues to operate primarily after legal violations occur rather than functioning as a continuous governance mechanism capable of preventing legal risks throughout the electronic health data lifecycle. These findings demonstrate the necessity for comprehensive legal reconstruction rather than incremental legislative revision.

2. Comparative Analysis of Electronic Health Data Protection

The normative evaluation demonstrates that Indonesia possesses a substantial legal foundation for protecting electronic health data. Nevertheless, several governance issues remain unresolved, particularly those relating to sector-specific regulation, institutional coordination, cybersecurity standards, patients' rights, and emerging digital technologies (Villalba-Mora et al., 2017). Comparative legal analysis therefore serves to identify regulatory approaches that have proven effective under other legal systems while assessing their relevance for strengthening Indonesia's electronic health data governance.

The European Union regulates electronic health data primarily through the General Data Protection Regulation (GDPR), which recognizes health information as a special category of personal data requiring a higher level of legal protection. Processing of such information is generally prohibited unless supported by explicit legal grounds, including explicit consent, public health interests, scientific research, or healthcare services authorized by law (Lestari et al., 2024). The GDPR also establishes comprehensive obligations concerning accountability, transparency, data minimization, purpose limitation, storage limitation, and integrity of personal data. These principles create a preventive legal framework that emphasizes risk management before personal data processing occurs rather than relying solely upon sanctions after violations take place.

Another significant characteristic of the GDPR concerns institutional supervision. Each Member State appoints an independent supervisory

authority responsible for monitoring compliance, conducting investigations, imposing administrative sanctions, and protecting data subjects' rights. This institutional arrangement creates legal certainty because supervisory authority is clearly allocated and supported by standardized enforcement mechanisms (Lalova-Spinks et al., 2024). The GDPR also requires Data Protection Impact Assessments for high-risk processing activities, mandatory breach notification procedures, and strict legal requirements governing international transfers of personal data. Collectively, these mechanisms establish an integrated governance model capable of protecting electronic health information throughout its entire processing cycle.

The United States adopts a different regulatory approach through the Health Insurance Portability and Accountability Act (HIPAA). Rather than regulating personal data generally, HIPAA establishes a sector-specific legal framework dedicated exclusively to healthcare information. Protected Health Information (PHI) receives legal protection through detailed administrative, technical, and physical safeguards that healthcare providers, health plans, and business associates must implement (Saka & Das, 2025). HIPAA also introduces standardized security rules, privacy rules, and breach notification requirements specifically designed for healthcare institutions. Such arrangements recognize that electronic health information possesses unique characteristics requiring regulatory standards beyond those applicable to ordinary personal data.

Comparison between Indonesia, the European Union, and the United States reveals several important differences. Indonesia has adopted

comprehensive legislation governing personal data protection and digital healthcare services, yet existing regulations continue to operate through separate legal regimes. Unlike the GDPR, Indonesian legislation has not established detailed legal standards governing high-risk processing activities, international health data transfers, or mandatory impact assessments for sensitive electronic health information. Unlike HIPAA, Indonesia has not introduced sector-specific cybersecurity obligations, standardized compliance requirements, or comprehensive administrative safeguards exclusively applicable to healthcare institutions (Cochlin et al., 2024). These differences indicate that Indonesia's principal challenge concerns regulatory integration rather than legislative availability.

The comparative analysis also demonstrates that successful electronic health data protection depends upon the integration of legal norms, institutional governance, technological safeguards, and effective supervision. The GDPR emphasizes fundamental rights through comprehensive personal data governance, whereas HIPAA prioritizes operational security and institutional compliance within the healthcare sector. Although both legal regimes employ different regulatory strategies, each establishes a coherent governance structure supported by clearly defined institutional responsibilities, preventive compliance mechanisms, and effective enforcement procedures. These common characteristics are not yet fully reflected within Indonesia's current legal framework, which continues to separate personal data regulation, healthcare administration, electronic systems governance, and cybersecurity into distinct regulatory sectors.

The comparative findings therefore confirm that future legal reform should extend beyond statutory amendment. Strengthening electronic health data protection requires an integrated governance model capable of harmonizing legal substance, institutional arrangements, technological safeguards, patients' rights, and supervisory mechanisms. These findings provide the analytical foundation for the subsequent section, which formulates a legal reconstruction designed to overcome the structural limitations identified through both the normative evaluation and comparative legal analysis.and good governance.

3. Legal Reconstruction of Electronic Health Data Protection

The normative evaluation and comparative legal analysis demonstrate that the principal challenge confronting Indonesia's electronic health data protection framework does not originate from legislative absence but from the absence of an integrated legal governance model capable of responding to technological transformation (Freye & Buchner, 2024). Existing legislation establishes important legal foundations for personal data protection and digital healthcare services; however, regulatory provisions continue to operate independently, producing fragmented governance, inconsistent institutional responsibilities, and uneven legal standards governing electronic health data. These findings indicate that strengthening legal protection requires a comprehensive legal reconstruction rather than isolated statutory amendments.

Legal reconstruction refers to a systematic process of reorganizing existing legal norms into a coherent normative framework capable of

achieving constitutional objectives more effectively. Such reconstruction does not merely introduce new legislation or replace existing regulations. Instead, it reorganizes legal substance, institutional arrangements, and regulatory mechanisms so that every component operates coherently and supports the same legal objectives (Moutaouakkil, 2025). Consequently, legal reconstruction aims to eliminate normative inconsistency while improving legal certainty, institutional accountability, and protection of fundamental rights.

The necessity for legal reconstruction becomes evident when existing legal theories are examined against contemporary digital health governance. Philipus M. Hadjon's theory of legal protection distinguishes preventive legal protection from repressive legal protection. Preventive protection seeks to prevent legal disputes through clear legal norms, administrative supervision, and effective regulatory mechanisms, whereas repressive protection provides remedies after legal violations have occurred (Naef, 2024). This theoretical distinction remains highly relevant for protecting individual rights. Nevertheless, rapid technological development has fundamentally changed the nature of legal risks associated with electronic health information. Artificial intelligence, cloud computing, interoperability, genomic databases, and cross-border electronic data exchange create continuous legal risks that extend beyond the traditional preventive and repressive framework (Wanjihia et al., 2024). Effective legal protection therefore requires continuous governance capable of accompanying every stage of electronic health data processing rather than operating only before or after legal disputes arise.

Lawrence Friedman's Legal System Theory also provides an important analytical foundation by explaining that legal effectiveness depends upon the interaction between legal substance, legal structure, and legal culture. This framework successfully explains why legislation alone cannot guarantee legal effectiveness without institutional support and public compliance. However, digital health governance introduces additional elements that cannot be fully accommodated through those three components alone (Chan et al., 2024). Cybersecurity standards, digital risk management, algorithmic accountability, electronic interoperability, and patients' digital autonomy have become fundamental components of electronic health data protection. Their strategic role extends beyond conventional legal substance and institutional structure because each directly determines whether sensitive health information remains secure, confidential, and lawfully processed throughout its lifecycle.

Hans Kelsen's theory of normative hierarchy and Ronald Dworkin's concept of law as integrity further reinforce the need for legal reconstruction. Kelsen emphasizes that every legal norm should operate consistently within a unified legal system, whereas Dworkin argues that legal interpretation should produce coherent principles rather than fragmented statutory provisions (Ladeia & Pereira, 2025). Evaluation of Indonesia's regulatory framework demonstrates that constitutional guarantees concerning privacy and healthcare have not yet been translated into an integrated governance structure governing electronic health data. Sectoral regulations continue to function separately, creating inconsistencies that reduce legal certainty and weaken effective protection of patients' rights. These theoretical

considerations demonstrate that the principal issue concerns regulatory coherence rather than legislative quantity.

Building upon these theoretical foundations, this study argues that legal protection for electronic health data requires conceptual development beyond existing legal protection scholarship. The proposed reconstruction does not reject classical legal protection theory but extends its application to digital governance. Legal protection should no longer be understood exclusively as preventive and repressive legal measures (Haleem et al., 2021). Instead, legal protection should operate as an integrated governance system combining normative regulation, institutional coordination, technological safeguards, protection of individual rights, and effective supervision throughout the entire lifecycle of electronic health data. Such reconstruction reflects the characteristics of digital health ecosystems, where legal protection must continuously accompany data collection, storage, processing, exchange, secondary use, and deletion.

Accordingly, the principal theoretical contribution of this research lies in the development of the Five-Pillar Legal Protection Model as a contemporary legal protection framework specifically designed for electronic health data governance. Unlike previous studies that primarily recommend regulatory harmonization or institutional reform, the proposed model reorganizes legal protection into five mutually integrated normative components that collectively strengthen legal certainty, cybersecurity resilience, institutional accountability, and protection of patients' rights. The model therefore represents an expansion of legal protection theory rather than

a compilation of policy recommendations because each pillar originates from the synthesis of normative findings, comparative legal analysis, and established legal theories.

The proposed reconstruction also contributes to contemporary legal scholarship by repositioning legal protection as a continuous governance mechanism. Conventional legal protection generally focuses on preventing legal violations or resolving disputes after violations occur. Electronic health data governance requires a broader legal architecture capable of anticipating technological risks before they materialize while ensuring accountability throughout every stage of digital health services. Consequently, legal protection evolves from a reactive legal concept into an integrated governance model capable of responding to technological innovation without compromising constitutional rights, legal certainty, or public trust. This reconstructed understanding provides the theoretical foundation for formulating the Five-Pillar Legal Protection Model presented in the following section.

4. Five-Pillar Legal Protection Model for Electronic Health Data Governance

The legal reconstruction developed through this research culminates in the formulation of the Five-Pillar Legal Protection Model, an integrated normative framework designed to strengthen electronic health data governance in Indonesia. The model emerges from the synthesis of three analytical stages conducted throughout this research (Haleem et al., 2021). Normative evaluation identifies the structural weaknesses of Indonesia's

current legal framework, comparative legal analysis demonstrates internationally recognized regulatory standards, and theoretical analysis reveals the limitations of existing legal protection theories when applied to digital health governance. Consequently, the Five-Pillar Legal Protection Model should be understood as a normative reconstruction that integrates legal protection theory with contemporary digital governance rather than merely proposing additional regulatory reform.

The model consists of five interrelated pillars that operate as a unified legal governance system. Each pillar performs a distinct normative function while simultaneously supporting the effectiveness of the remaining pillars. Legal substance establishes the normative foundation governing electronic health data, institutional governance ensures effective implementation of legal norms, cybersecurity integration protects the confidentiality and integrity of electronic health information, patients' rights protection guarantees individual autonomy over personal health data, and oversight together with law enforcement secures regulatory compliance through continuous supervision and proportionate sanctions (Jain, 2023). The effectiveness of the proposed model therefore depends upon the interaction of all five pillars rather than the implementation of any single component.

The first pillar, Legal Substance Reform, addresses the absence of a coherent legal framework governing electronic health data. Normative evaluation demonstrates that existing legislation regulates personal data protection, healthcare services, electronic systems, and medical records through separate legal instruments that frequently operate independently

(Gadola et al., 2026). Such conditions create inconsistencies concerning emerging technologies, including artificial intelligence, cloud-based health information systems, interoperability, genomic information, and international health data transfers. Legal reconstruction therefore requires harmonization of existing legislation through sector-specific provisions that establish comprehensive legal standards governing the entire lifecycle of electronic health data. This pillar extends beyond legislative amendment by ensuring normative consistency among constitutional guarantees, statutory provisions, and implementing regulations.

The second pillar, Institutional Governance, responds to fragmented administrative authority identified during the normative evaluation. Effective legal protection requires clearly defined institutional responsibilities supported by structured coordination among public authorities responsible for healthcare regulation, personal data protection, and cybersecurity. Integrated governance improves regulatory consistency, accelerates incident response, strengthens accountability, and reduces administrative uncertainty. Institutional governance therefore functions as the operational mechanism translating legal norms into effective implementation while ensuring that regulatory responsibilities remain clearly allocated throughout the electronic health data governance system.

The third pillar, Cybersecurity Integration, reflects the recognition that electronic health data cannot be adequately protected through conventional legal regulation alone. Comparative analysis demonstrates that internationally recognized regulatory systems incorporate technical safeguards as an

essential component of legal governance. Consequently, cybersecurity should be recognized as an autonomous legal pillar rather than merely a technical obligation. Comprehensive protection requires mandatory encryption, access control, authentication procedures, continuous security monitoring, audit mechanisms, risk assessment, incident response protocols, and regular cybersecurity evaluation. Such safeguards ensure that legal protection accompanies technological development without compromising the confidentiality, integrity, and availability of electronic health information.

The fourth pillar, Patients' Rights Protection, strengthens the human rights orientation of electronic health data governance. Conventional regulatory approaches frequently emphasize institutional obligations while providing limited attention to patients as rights holders. The reconstructed model places patients at the centre of digital health governance by recognizing enforceable rights relating to informed consent, access to personal medical information, correction of inaccurate records, withdrawal of consent, restriction of data processing, transparency, and timely notification following data breaches. Recognition of these rights transforms patients from passive providers of medical information into active legal subjects possessing meaningful control over the processing of electronic health data.

The fifth pillar, Oversight and Law Enforcement, ensures the effectiveness of the entire governance framework through continuous supervision and accountable enforcement. Effective legal protection cannot rely solely upon statutory obligations without corresponding monitoring and compliance mechanisms. Oversight therefore includes periodic regulatory

audits, compliance evaluation, cybersecurity supervision, breach reporting, and coordinated institutional review. Law enforcement complements these preventive mechanisms through administrative, civil, and criminal sanctions proportionate to the seriousness of legal violations. Continuous supervision strengthens institutional accountability while increasing public confidence in digital healthcare services.

The Five-Pillar Legal Protection Model differs fundamentally from previous approaches proposed in legal scholarship. Earlier studies generally concentrated on individual aspects of electronic health data governance, including privacy protection, electronic medical records, information security, or regulatory harmonization. The present model integrates those individual dimensions into a single normative framework grounded in legal protection theory, legal system theory, normative coherence, and comparative legal analysis. This integration enables electronic health data governance to operate through a coherent legal architecture capable of responding to technological innovation while preserving constitutional guarantees and legal certainty.

The theoretical contribution of the proposed model lies in its reconceptualization of legal protection as a continuous governance mechanism rather than a legal response activated only before or after legal violations occur. Classical legal protection theory distinguishes preventive and repressive legal protection, whereas the Five-Pillar Legal Protection Model extends those concepts by introducing integrated governance throughout every stage of electronic health data processing. Protection

therefore accompanies data collection, storage, processing, exchange, secondary use, retention, and deletion through mutually reinforcing legal, institutional, technological, and supervisory mechanisms. This conceptual development expands existing legal protection scholarship by demonstrating that digital health governance requires continuous normative integration rather than isolated legal safeguards.

Accordingly, the Five-Pillar Legal Protection Model represents the principal contribution of this research to contemporary legal scholarship. The model offers not merely a legislative recommendation but a reconstructed legal protection framework capable of integrating constitutional principles, legal certainty, technological governance, institutional accountability, and patients' rights into a coherent normative system. Such reconstruction provides a theoretical foundation for future legal reform concerning electronic health data protection while supporting the sustainable development of Indonesia's digital health ecosystem.

D. CONCLUSION

Indonesia has established a substantial legal foundation for protecting electronic health data through constitutional provisions and sectoral legislation; however, the existing framework remains characterized by regulatory inconsistency, fragmented governance, limited institutional coordination, and inadequate legal standards for emerging digital health technologies. The normative and comparative analyses demonstrate that strengthening legal protection requires comprehensive legal reconstruction rather than incremental legislative amendment. This study therefore proposes the Five-Pillar Legal

Protection Model, comprising Legal Substance Reform, Institutional Governance, Cybersecurity Integration, Patients' Rights Protection, and Oversight and Law Enforcement, as an integrated normative framework for electronic health data governance. Unlike previous studies that primarily recommend regulatory harmonization, the proposed model expands legal protection scholarship by reconstructing classical legal protection theory into a continuous governance framework capable of integrating legal norms, institutional accountability, technological safeguards, and patients' rights. This model provides both a theoretical foundation for the future development of digital health law and a normative reference for legal reform supporting secure, accountable, and sustainable digital healthcare in Indonesia.

REFERENCES

Akkhateerathitiphum, R. A. R. (2026). Toward Fairness in Digital Consumer Protection: A Comparative Legal and Socio-Regulatory Perspective on Digital Platform Governance. *Frontiers in Sociology*, *11*. https://doi.org/10.3389/fsoc.2026.1828884

Benseghir, M., Bentria, M., Zerara, A., & Bendriss, H. (2025). Legal Guarantees for the Protection of Patient Confidentiality: A Cross-Jurisdictional Study. *LAW REFORM*, *22*(1), 82–112. https://doi.org/10.14710/lr.v22i1.65728

Benseghir, M., Bentria, M., Zerara, A., Bendriss, H., & Berrahlia, B. (2025). Toward an Effective Legal Framework for Digital Health E-Commerce: Insights from the UAE and Indonesia. *Lex Scientia Law Review*, *9*(2), 1668–1700. https://doi.org/10.15294/lslr.v9i2.12152

Benseghir, M., Zerara, A., Bentria, M., Bendriss, H., & Muhtar, M. H. (2025). Legal Aspects of Patient Data Governance in Digital Health: A Comparative Analytical Study of UAE and Indonesian Legislation. *Journal of Indonesian Legal Studies*, *10*(2). https://doi.org/10.15294/jils.v10i2.10025

Chan, H. Y. (2026). Legal Preparedness in Implementing Digital Contact Tracing Apps in Managing Public Health Threats: The Singapore Experience. *International Journal of Law in Context*, *22*(1), 60–74.

Chan, H. Y., Toh, H. J., & Lysaght, T. (2024). Cross-Jurisdictional Data Transfer in Health Research: Stakeholder Perceptions on the Role of Law. *Asian Bioethics Review*, *16*(4), 663–682. https://doi.org/10.1007/s41649-024-00283-8

Cochlin, F. J., Curran, C. D., & Schmit, C. D. (2024). Unlocking Public Health Data: Navigating New Legal Guardrails and Emerging AI Challenges. *Journal of Law, Medicine and Ethics*, *52*(2), 252–264.

De Anna, G. L. (2022). The International Data Governance Landscape for Biomedical

Research. *Journal of Law and the Biosciences*, *9*(1), lsac005. https://doi.org/10.1093/jlb/lsac005

Fauziah, Y. A., Susanto, D. A., & Utama, Y. P. (2025). Legal Protection of Patient's Health Data in the Digital Era. *Jurnal Hukum Dan Etika Kesehatan*, *6*(1). https://doi.org/10.30649/jhek.v6i1.270

Freye, M., & Buchner, B. (2024). Legal Regulation of Digital Public Health Interventions—Hindrance or Stimulus? *Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz*, *67*(3), 285–291. https://doi.org/10.1007/s00103-024-03835-3

Gadola, S., Pek, S., Trabucchi, D., & Buganza, T. (2026). More than Just Digital Platforms: A Framework to Uncover the Characteristics of Platform Cooperatives through Platform Business Models. *Technological Forecasting and Social Change*, *229*, 124725. https://doi.org/10.1016/j.techfore.2026.124725

Greenhalgh, T., Wherton, J., Shaw, S., & Morrison, C. (2020). Video Consultations for COVID-19 and Beyond: Lessons for Digital Health Policy and Regulation. *Journal of Medical Internet Research*, *22*(8), e19323. https://doi.org/10.2196/19323

Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Telemedicine for Healthcare: Capabilities, Features, Barriers, and Applications. *Sensors International*, *2*, 100117. https://doi.org/10.1016/j.sintl.2021.100117

Hutchinson, T., & Duncan, N. (2017). Defining and Describing What We Do: Doctrinal Legal Research. *Deakin Law Review*.

Jain, K. (2023). Digital Health Governance: Legal and Ethical Challenges in the Era of Artificial Intelligence. *Journal of Health Organization and Management*, *37*(8), 1023–1041. https://doi.org/10.1108/JHOM-02-2023-0057

Jawed, M., & Girish, R. (2026). Digital Constitutionalism and Platform Governance: Rethinking Rights and Regulation in India's Social Media Ecosystem. *Journal of Media Law*. https://doi.org/10.1080/17577632.2026.2660478

Kusuma, H., Agustina, D., & Santoso, B. (2022). Personal Data Protection in Indonesian Electronic Health Services: Legal Challenges and Future Directions. *International Journal of Electronic Healthcare*, *14*(2), 145–162. https://doi.org/10.1504/IJEH.2022.126118

Ladeia, Y. R., & Pereira, D. M. (2025). Law-Based and Standards-Oriented Approach for Privacy Impact Assessment in Medical Devices: A Topic for Lawyers, Engineers and Healthcare Practitioners in MedTech. *Computer Law and Security Review*.

Lalova-Spinks, T., Valcke, P., & Ioannidis, J. P. A. (2024). EU–US Data Transfers: An Enduring Challenge for Health Research Collaborations. *Npj Digital Medicine*, *7*, 215. https://doi.org/10.1038/s41746-024-01205-6

Lestari, R., Prasetyo, D., & Nugroho, A. (2024). Legal and Technological Framework for Electronic Health Records in Indonesia. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(2), 100281. https://doi.org/10.1016/j.joitmc.2024.100281

Mardiansyah, R., Makarim, E., & Sulistyowati. (2025). Legal Framework Chamber of Governance Digital Health Innovation: Insights from Implementation of Health Technology Transformation in Indonesia. *International Journal of Public Law and Policy*.

Moutaouakkil, A. (2025). Safeguarding Patient Privacy in eHealth Systems: Bridging

Theory and Practice through a Scoping Review and Healthcare Survey. *BMC Medical Informatics and Decision Making*, *25*, 126. https://doi.org/10.1186/s12911-025-02931-7

Muhaimin. (2023). Reconstructing Normative Legal Research: Contemporary Approaches to Legal Interpretation. *Fiat Justisia: Jurnal Ilmu Hukum*, *17*(2), 155–172. https://doi.org/10.25041/fiatjustisia.v17no2.3077

Naef, F. (2024). The Anonymous Data Warehouse: A Hands-On Framework for Anonymizing Data from Digital Health Applications. *Cureus*, *16*(4), e57546. https://doi.org/10.7759/cureus.57546

Putri, M. S. (2026). Rule of Law and Legal Pluralism in Indonesia: Constitutional Transformation, Regulatory Governance, and Rights Protection in a Decentralized State. *Indonesian Journal of Law, Governance, and Regulation*, *1*(1).

Saka, S., & Das, S. (2025). Evaluating Privacy Measures in Healthcare Apps Predominantly Used by Older Adults. *Proceedings on Privacy Enhancing Technologies*.

Salami, E. (2022). Implementing the AfCFTA Agreement: A Case for the Harmonization of Data Protection Law in Africa. *Journal of African Law*, *66*(2), 281–291. https://doi.org/10.1017/S0021855322000110

Salami, E. (2024). Cross-Border Data Transfer between the GCC Data Protection Laws and the GDPR. *Global Journal of Comparative Law*, *13*(2), 178–200. https://doi.org/10.1163/2211906X-13020003

Sekalala, S., Andanda, P., & Chatikobo, T. (2026). Regulating Digital Health in the Global South: Critical and Decolonial Approaches. *International Journal of Law in Context*, *22*(1), 1–10. https://doi.org/10.1017/S1744552325100335

Shabani, M., & Yilmaz, S. (2022). Lawfulness in Secondary Use of Health Data: Interplay between Three Regulatory Frameworks of GDPR, DGA & EHDS. *Technology and Regulation*, 128–134. https://doi.org/10.26116/techreg.2022.013

Smit, J.-A. R., Mostert, M., van der Graaf, R., Grobbee, D. E., & van Delden, J. J. M. (2024). Specific Measures for Data-Intensive Health Research without Consent: A Systematic Review of Soft Law Instruments and Academic Literature. *European Journal of Human Genetics*, *32*(1), 21–30. https://doi.org/10.1038/s41431-023-01471-0

Smits, J. M. (2021). Comparative Law and Methodology: Contemporary Developments in Functional Legal Comparison. *Maastricht Journal of European and Comparative Law*, *28*(6), 765–781. https://doi.org/10.1177/1023263X211048930

Van Hoecke, M. (2018). Legal Doctrine: Which Method(s) for What Kind of Discipline? *Methods of Legal Research*, *12*(1), 1–18.

van Kolfschooten, H., Parwani, P., & Perehudoff, K. (2026). Accounting for EU External Effects: From Clinical Trials to Data Colonialism to AI Ethics Dumping. *International Journal of Law in Context*, *22*(1), 45–59.

Villalba-Mora, E., Casas, M., Lupiañez-Villanueva, M., & Maghiros, F. (2017). Adoption of Digital Health Technologies and Regulatory Challenges: A European Perspective. *Journal of Medical Internet Research*, *19*(11), e367. https://doi.org/10.2196/jmir.8773

Wanjihia, V. W., Muriithi, B. K., & Kaneko, S. (2024). A Scoping Overview of Global Legislation on Data Privacy and Protection: What Are the Implications for Data

Use, Transfer, and Sharing in e-Health Research? *Austin Public Health*, *8*(1), 1023.

Wulandari, P. (2025). Normative Legal Research Methodology from the Experts' Perspective: A Comparative Analysis of Concepts and Approaches. *Archipel: Journal of Indonesian Interdisciplinary Studies*, *1*(6), 1–18. https://doi.org/10.65739/archipel.v1i6.34