E-ISSN: 2963-2900 | P-ISSN: 2964-9048
https://jmi.rivierapublishing.id/
Volume 4 Number 4 April 2025
JMI Jurnal Multidisiplin Indonesia

Telemedicine Regulation in Indonesia: Legal Frameworks, Challenges, and Future Directions

Fifi Mutiah*, Hotma Sibuea, Mardi Candra
Universitas Jayabaya, Indonesia
Correspondence: fimut273@gmail.com*

Abstract

The rapid advancement of digital technology has positioned telemedicine as a transformative solution to address healthcare disparities, particularly in geographically fragmented regions like Indonesia. Despite its potential, telemedicine adoption in Indonesia faces significant challenges, including regulatory ambiguities, inadequate infrastructure, and concerns over data security and professional accountability. While recent legal frameworks, such as Law No. 17 of 2023 and Government Regulation No. 28 of 2024, aim to address these issues, their implementation remains inconsistent, risking patient safety and trust. This study fills critical gaps in existing literature by integrating the rule of law and health justice frameworks to evaluate Indonesia's telemedicine regulations—a novel approach absent in prior works. The study addresses two key research questions: (1) How does Indonesia's current legal framework regulate telemedicine, and what gaps exist in practice? (2) How can telemedicine regulations align with the principles of a legal state (Rechtsstaat) to ensure accountability and equity? Employing a normative juridical methodology, the research combines legislative analysis, conceptual evaluation, and case studies, including the Dr. Damar case (2021), to assess regulatory coherence. Findings reveal significant gaps, including unclear liability standards for misdiagnoses, weak enforcement of data privacy laws, and disparities in rural telemedicine access. The study highlights misalignments with international standards like the GDPR and HIPAA, particularly in AI governance and cross-border data flows. To address these issues, the study recommends: (1) strengthening operational standards by adopting WHO guidelines and mandating AI validation; (2) clarifying liability frameworks to define malpractice accountability; and (3) bridging the digital divide through subsidized internet and device programs.

Keywords: telemedicine, regulatory gaps, health justice, data privacy in Indonesia.

Corresponding Author: Fifi Mutiah
E-mail: fimut273@gmail.com

INTRODUCTION

The rapid evolution of digital technology has ushered in transformative changes in healthcare delivery, with telemedicine emerging as a pivotal innovation to address disparities in access, particularly in geographically fragmented regions like Indonesia. Telemedicine has revolutionized healthcare by enabling remote consultations, diagnoses, and treatment, particularly in underserved regions. In Indonesia, a vast archipelago with significant disparities in healthcare access, telemedicine offers a promising solution to improve equity (O, 2010). However, its adoption is hindered by regulatory ambiguities,

inadequate infrastructure, and concerns over data security and professional accountability (Setiawati, 2023). The Indonesian government has introduced legal frameworks, such as Law No. 17 of 2023 and Government Regulation No. 28 of 2024, to address these challenges. Yet, the alignment between these regulations and on-the-ground implementation remains inconsistent, risking patient safety and trust (Rahma & Supriyadi, 2021).

Existing literature on telemedicine in Indonesia has predominantly focused on technological adoption and operational challenges. For instance, Widyaningrum & Nugroho (2020) examined IoT-based remote patient monitoring in Indonesian hospitals, highlighting technical barriers but overlooking legal safeguards. Similarly, (Smith, 2024a) analyzed AI integration in telemedicine platforms but did not address regulatory gaps in liability for misdiagnoses. Other studies, such as Mulyani and Setiawan (2023), explored data privacy issues but limited their scope to generic compliance with Indonesia's Personal Data Protection Law (No. 27 of 2022), without delving into telemedicine-specific vulnerabilities.

This paper fills critical gaps by: Legal-Theoretical Integration: Applying the rule of law and health justice frameworks to evaluate Indonesia's telemedicine regulations—a lens absent in prior works. Case-Based Analysis: Examining unresolved legal disputes, such as the 2021 Dr. Damar case, where a telemedicine misdiagnosis led to patient harm but exposed ambiguities in liability under Law No. 17 of 2023. Regulatory Synergy: Proposing actionable steps to harmonize telemedicine operations with Indonesia's data security laws (e.g., PDP Law) and international standards like GDPR. There for the emphasizing the novelty of integrating theories of the rule of law, health justice, and accountability to evaluate Indonesia's regulatory framework. Research objectives are; (1) to analyze the legal framework for telemedicine in Indonesia and its implementation challenges, and (2) to propose recommendations for strengthening regulatory coherence and accountability in telemedicine services.

RESEARCH METHODS

This study adopts a normative juridical approach, emphasizing an analysis of legislation, legal concepts, and case studies (Marzuki, 2017). The research relies on primary legal materials, including Law No. 17 of 2023 on Financial Sector Development and Government Regulation No. 28 of 2024 concerning Digital Financial Services. Secondary legal materials consist of academic articles, judicial decisions, legal commentaries, and relevant regulations. The legal interpretation methods used include grammatical, historical, systematic, and teleological interpretations to ensure a comprehensive analysis of the alignment between regulatory frameworks and practical needs within the fintech sector.

The population for this study comprises all laws and regulations related to fintech and cybersecurity in Indonesia. The data sample is selected purposively, focusing on regulations and case decisions from the period 2018–2024. The sampling technique utilized is purposive sampling, targeting sources that specifically address fintech

regulatory frameworks and cyber fraud cases. The main research instrument is a document study checklist developed based on legal doctrinal standards. The validity of data is ensured through triangulation by cross-referencing multiple sources, while reliability is maintained by systematic coding and classification of legal provisions and cases to ensure consistency in analysis.

The data collection technique includes systematic legal research and literature review, guided by a structured extraction form. The research procedure follows stages of data identification, selection, extraction, evaluation, and synthesis. The data analysis technique involves thematic analysis to identify key patterns and critical gaps in the regulatory and practical framework, providing a basis for proposing future improvements in fintech legal governance in Indonesia.

RESULTS AND DISCUSSION

Findings and Discussion on Regulatory Framework

The regulatory framework for telemedicine in Indonesia, as outlined in **Law No. 17 of** 2023 and Government Regulation No. 28 of 2024, establishes a foundational legal structure but reveals critical gaps in operational standards and technological adaptability. Below is a detailed discussion comparing these regulations with theoretical perspectives and empirical findings.

Law No. 17 of 2023: Mandating Telemedicine with Limited Operational Clarity

Article 172 of Law No. 17/2023 explicitly integrates telemedicine into healthcare services, emphasizing its role in bridging geographical disparities (Siregar, 2023). However, the law falls short in prescribing detailed operational standards, such as:

a) Technical requirements for telemedicine platforms (e.g., encryption standards, data storage protocols).
b) Quality assurance mechanisms to ensure diagnostic accuracy in virtual consultations (Rahmat & Dewi, 2021).
c) Liability frameworks for malpractice in telemedicine, particularly for misdiagnoses due to technological limitations (Suryaprawira et al., 2024).

Theoretical Gap: The law aligns with the rule of law principle by formalizing telemedicine but neglects the accountability theory Roberts (2014), which demands clear guidelines for practitioner responsibility and patient redress. For instance, it does not address whether liability rests with healthcare providers, platform operators, or AI developers in cases of errors (Smith, 2024b).

Government Regulation No. 28 of 2024: Infrastructure Focus vs. Technological Advancements

a. Article 559 of Government Regulation No. 28/2024 outlines infrastructure requirements (e.g., secure servers, interoperable systems) but omits critical aspects of emerging technologies:

   AI-driven diagnostics: The regulation does not specify validation protocols for AI tools used in telemedicine, risking unreliable diagnoses (Smith et al., 2024).

For example, Babylon Health's AI misdiagnosis cases in the UK (Smith, 2024) highlight the need for algorithmic transparency and audit trails.

IoT integration: While remote monitoring devices (e.g., wearable sensors) are increasingly used, the regulation lacks standards for data accuracy or device certification (Widyaningrum & Nugroho, 2020).

Theoretical Gap: The regulation reflects a technological determinism approach, assuming infrastructure alone ensures efficacy. However, social contract theory Johnson & Brown (2018)**argues** that regulations must also build public trust by addressing ethical risks (e.g.,AI bias, data misuse).

Comparative Analysis with International Frameworks

a. EU's GDPR and HIPAA in the U.S. mandate stringent data protection and patient consent mechanisms, whereas Indonesia's framework lacks equivalent specificity (Setiawati, 2023). For example:

GDPR's Article 22 restricts fully automated decision-making in healthcare, a provision absent in Indonesian law (Tikkinen-Piri et al., 2018).

HIPAA's Security Rule enforces encryption standards for e-health records, while Indonesia's reliance on Law No. 27/2022 on PDP (Personal Data Protection) remains untested in telemedicine contexts ((Rahmat & Dewi, 2021).

Given these challenges, the following regulatory enhancements are proposed to align Indonesia's telemedicine framework with global standards while addressing local gaps. To bridge the divide between current regulations and evolving telemedicine needs, three strategic interventions should be prioritized on targeted reforms—particularly in operational standards, AI governance, and stakeholder collaboration—as outlined below:"

- Operational Standards: Adopt WHO's telemedicine guidelines (WHO, 2010) to standardize consent protocols, data security, and practitioner training.
- AI Regulation: Introduce algorithmic accountability clauses requiring validation of AI tools by Indonesia's Ministry of Health (Smith et al., 2024).
- Stakeholder Collaboration: Establish a regulatory sandbox (Kemenkes RI, 2022) to pilot innovations like IoT-based monitoring while mitigating risks.

Findings and Discussion: Challenges and Theoretical Alignment in Indonesia's Telemedicine Framework

1. Challenges in Telemedicine Implementation

Data Privacy Concerns

Despite the enactment of Indonesia's Personal Data Protection Law (No. 27 of 2022), enforcement remains weak, leading to persistent vulnerabilities in telemedicine platforms (Mulyani & Setiawan, 2023). Key issues include:Inadequate Encryption Standards: Many platforms lack end-to-end encryption, exposing sensitive patient data to breaches (Kern et al., 2020).

Third-Party Data Sharing: Some telemedicine providers share patient data with pharmaceutical or insurance companies without explicit consent, violating Article 4(2) of the PDP Law (Mulyani & Setiawan, 2023).

Lack of Oversight: Unlike the EU's GDPR or HIPAA in the U.S., Indonesia has no dedicated agency to audit compliance, allowing loopholes in data security (Tikkinen-Piri et al., 2018).

Theoretical Gap:

Rule of Law Principle Suryadi (2021a) demands clear legal safeguards and strict penalties for violations, yet Indonesia's framework lacks specific sanctions for telemedicine-related breaches.

Accountability Theory (Roberts, 2014) highlights the need for transparent data governance, yet enforcement mechanisms remain underdeveloped.

Accountability and Legal Ambiguities

Telemedicine introduces unique liability challenges, particularly in misdiagnosis cases where responsibility is unclear (Rahayu, 2023).

Key problems include:

Unclear Liability Standards: If an AI-driven diagnosis tool (e.g., Babylon Health's case in the UK) provides incorrect advice, it is unclear whether the doctor, platform developer, or hospital is legally responsible (Smith et al., 2024).

Informed Consent Gaps: Many patients do not fully understand telemedicine risks, leading to disputes over malpractice (Rahmat & Dewi, 2021).

Jurisdictional Issues: Cross-border telemedicine (e.g., Indonesian patients consulting foreign doctors) lacks legal clarity on which country's laws apply (Suryaprawira et al., 2024).

Theoretical Gap:

Social Contract Theory (Johnson & Brown, 2018) suggests that laws should protect both patients and providers, yet Indonesia's regulations fail to define malpractice liability in virtual care.

Professional Ethics Doctrine Beauchamp & Childress (2019) requires clear guidelines for telemedicine practitioners, but current laws do not specify ethical obligations (e.g., ensuring accurate digital diagnoses).

2. Theoretical Alignment (and Misalignment) in Indonesia's Telemedicine Policies
   a. Rule of Law Principle: Protection vs. Implementation

      Principle: The rule of law Suryadi (2021b) requires predictable, transparent regulations to ensure fairness.

Reality: While Law No. 17/2023 and PP No. 28/2024 establish telemedicine legality, they lack:

Standardized operational procedures (e.g., mandatory audit logs for AI diagnostics).

Judicial remedies for patients harmed by telemedicine errors (Rahayu, 2023).

Example: Unlike Australia's Telehealth Law, which mandates real-time monitoring of remote consultations, Indonesia's laws remain vague on quality control (Hughes & Edwards, 2020a).

b. Health Justice Theory: Equity vs. Digital Divide

Principle: Health justice Tanagho (2008) demands equal access to healthcare, including telemedicine.

Reality: Indonesia faces geographical disparities: Urban vs. Rural Access: Only 35% of rural clinics have stable internet, limiting telemedicine adoption (Wahyudi, 2023).

Affordability Issues: Low-income patients often cannot afford smartphones or data plans needed for teleconsultations (Rahma & Supriyadi, 2021).

Example: Brazil's Telemedicine Program subsidizes internet costs for rural patients—a policy Indonesia has not yet adopted (Pereira & Ramesh, 2020).

To reconcile these challenges with the theoretical imperatives of equity, accountability, and legal certainty, the following policy interventions are proposed Addressing Indonesia's telemedicine gaps requires immediate action on three fronts: robust data governance, clarified liability structures, and equitable access—each detailed below:

- Strengthen Data Protection
  Establish a dedicated health data authority (similar to the U.S. OCR under HIPAA) to enforce PDP Law compliance (Mulyani & Setiawan, 2023).
- Clarify Liability Frameworks:
  Amend Law No. 17/2023 to define malpractice liability in telemedicine (Rahayu, 2023).
- Bridge the Digital Divide:
  Expand universal internet coverage and subsidize telemedicine devices for rural areas (Daniels, 2008).

Telemedicine Challenges in Indonesia: Case Examples and Regulatory Gaps Misdiagnosis and Liability Issues

The Dr. Damar Case (2021): Accountability in Virtual Diagnoses In 2021, Dr. Damar, an Indonesian physician, faced legal action after a teleconsultation misdiagnosis led to severe patient complications (Suryaprawira et al., 2024).

The case exposed critical flaws in remote diagnostics:
Limited Physical Examinations: The patient's symptoms (initially diagnosed as a minor infection via video call) were later confirmed as acute appendicitis after hospitalization (Rahayu, 2023). Legal Ambiguities: Indonesia's Medical Practice Law (No. 29/2004) does not explicitly address telemedicine malpractice, leaving courts to interpret liability (Rahmat & Dewi, 2021).

Systemic Risks in Patient-Reported Data

A 2023 study by Rahayu found that 40% of Indonesian telemedicine platforms lacked protocols to verify patient-submitted data (e.g., self-reported vitals), increasing misdiagnosis risks. Key gaps include:

No Standardized Triage: Unlike Australia's telehealth guidelines, which mandate structured symptom checklists, Indonesian providers often rely on unverified patient descriptions (Hughes & Edwards, 2020b).

Liability Loopholes: Current laws do not clarify whether doctors or platform operators bear responsibility for errors stemming from incomplete data ((Howson & Smith, 2008).

Data Privacy Breaches: Weak Enforcement and Compliance

a. The Alodokter Data Leak (2022)
   In 2022, Alodokter, a leading telemedicine platform, suffered a breach exposing 2.3 million patient records, including sensitive health data (Kompas, 2022). This incident highlighted:
   Encryption Failures: Despite Government Regulation No. 28/2024 (Article 559) requiring secure infrastructure, many platforms use outdated encryption (Mulyani & Setiawan, 2023).
   Insufficient Penalties: The PDP Law (No. 27/2022) imposes fines up to 2% of annual revenue, but enforcement remains rare compared to the EU's GDPR (Tikkinen-Piri et al., 2018).
b. Rural Clinics and Unsecured Communications
   WhatsApp Consultations: Rural clinics frequently use unencrypted messaging apps (e.g., WhatsApp) for telemedicine, violating PDP Law Article 36 on data minimization (Mulyani & Setiawan, 2023).
   Regulatory Blind Spots: No specific guidelines prohibit third-party apps for telehealth, unlike HIPAA's ban on SMS-based consultations in the U.S. (Kern et al., 2020).

Regulatory Fragmentation and AI Governance Gaps

a. Conflicting Laws and Standards
   Law No. 17/2023 mandates telemedicine integration but clashes with older rules like MoH Regulation No. 20/2019, which lacks interoperability requirements (Kemenkes, 2023b).
   Example: A hospital using two different platforms (e.g., Halodoc and SATUSEHAT) cannot share patient data seamlessly, risking treatment delays (Widyaningrum & Nugroho, 2020).

b. Unregulated AI Diagnostics
   Algorithmic Bias: AI tools used for diagnoses (e.g., skin cancer detection) are not audited for accuracy, risking racial or gender bias (Smith et al., 2024).
   No Liability Framework: Unlike the EU's AI Act, Indonesia has no rules holding AI developers accountable for diagnostic errors (Tikkinen-Piri et al., 2018).

Integration of Data Security and Privacy Regulations: Global Comparisons

1. Consent Mechanisms: Loopholes in Indonesian Law
   Implied Consent Risks: PDP Law Article 20 allows "implied consent" for health data, whereas GDPR Article 9 mandates explicit opt-ins (Mulyani & Setiawan, 2023).*Case Example*: A 2023 study found 60% of telemedicine users were unaware their data could be shared with advertisers (Rahmat & Dewi, 2021).
2. Cross-Border Data Flows: Enforcement Challenges
   Cloud Server Risks: Platforms like Halodoc use AWS Singapore servers, but PDP Law Article 48's data localization rules are weakly enforced (Kemenkes, 2023a).
   GDPR Contrast: The EU mandates Standard Contractual Clauses (SCCs) for cross-border transfers, but Indonesia lacks equivalent safeguards (Tikkinen-Piri et al., 2018).
3. Interoperability Failures
   SATUSEHAT Integration Gaps: Poor API compatibility between telemedicine apps and Indonesia's national health database creates data silos (Kemenkes, 2023). Global Benchmark: The U.S. 21st Century Cures Act penalizes providers for blocking data sharing, a policy Indonesia could adopt (Kern et al., 2020)

CONCLUSION

This study critically examines Indonesia's telemedicine regulatory framework in light of two research questions. First, it finds that despite the existence of Law No. 17/2023 and Government Regulation No. 28/2024, significant regulatory gaps persist. Operational standards, such as AI validation protocols, data encryption requirements, and clear liability assignments for telemedicine misdiagnoses, remain insufficiently regulated. Case examples such as Dr. Damar's misdiagnosis incident (2021) and the Alodokter data breach (2022) highlight real-world vulnerabilities, indicating weaknesses in enforcement and patient protection. Second, while the framework demonstrates partial alignment with the principles of Rechtsstaat—particularly regarding formal legal recognition of telemedicine services—it falls short in ensuring substantive rule of law principles such as accountability and equitable access. The lack of clear liability standards for AI-driven diagnoses and inadequate protections for patients in rural areas, especially regarding internet access, further weakens Indonesia's compliance with rule of law ideals. In comparison to stronger international benchmarks, such as the EU's GDPR framework and Australia's telehealth regulations, Indonesia's system lacks stringent consent mechanisms and cross-border data protection rules. Future research is suggested to explore the development of a comprehensive legal model that addresses AI-specific liabilities, strengthens cybersecurity regulations, and integrates international best practices to enhance telemedicine governance in Indonesia.

REFERENCES

Beauchamp, T. L., & Childress, J. F. (2019). *Principles of biomedical ethics* (8th ed.). Oxford University Press.

Daniels, N. (2008). *Just health: Meeting health needs fairly*. Cambridge University Press. https://doi.org/10.1017/CBO9780511800510

Howson, R., & Smith, K. (2008). *Hegemony: Studies in consensus and coercion* (Vol. 56). Routledge.

Hughes, P., & Edwards, R. (2020a). Telemedicine policy evolution: A case study of Australia and New Zealand. *Journal of Telemedicine and E-Health*, *26*(4), 45–58.

Hughes, P., & Edwards, R. (2020b). Telemedicine policy evolution: A case study of Australia and New Zealand. *Journal of Telemedicine and E-Health*, *26*(4), 45–58.

Johnson, L., & Brown, K. (2018). Social contract theory and its implications for democratic governance. *International Journal of Constitutional Law*, *16*(2), 234–250.

Kemenkes. (2023a). *Evaluasi implementasi SATUSEHAT*. Ministry of Health.

Kemenkes, R. I. (2023b). *Laporan tahunan transformasi digital kesehatan*. Kementerian Kesehatan Republik Indonesia.

Kern, L. M., Barron, Y., & Edwards, A. (2020). Privacy and security of health information in the digital era. *Journal of Medical Internet Research*, *22*(7), e17892. https://doi.org/10.2196/17892

Kompas. (2022). *Kebocoran data pasien Alodokter: Apa yang harus dilakukan?*

Mulyani, D., & Setiawan, Y. (2023). Data privacy and security in telemedicine services. *Journal of Health Informatics*, *5*(4), 45–56.

O, W. H. (2010). *Telemedicine: Opportunities and developments in member states*. WHO Press.

Pereira, L., & Ramesh, S. (2020). *Telemedicine policies in developing countries*. Health Policy Press.

Rahayu, S. (2023). Legal protection for healthcare workers in telemedicine services. *Indonesian Journal of Health Law*, *15*(2), 78–89.

Rahma, D., & Supriyadi, A. (2021). Affordability barriers in telemedicine adoption. *Indonesian Journal of Public Health*, *8*(2), 112–125.

Rahmat, B., & Dewi, S. (2021). Regulatory inconsistencies in Indonesian telemedicine. *Asian Journal of Health Law*, *14*(3), 45–60.

Roberts, M. (2014). *Accountability in healthcare*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198722498.001.0001

Setiawati, N. (2023). The urgency of comprehensive legal framework for telemedicine in Indonesia. *Journal of Law and Technology*, *7*(3), 213–230.

Siregar, R. A. (2023). *Health law in Indonesia: KUHP and health legislation*. Sinar Grafika.

Smith, J. (2024a). *AI misdiagnosis in telemedicine: Case studies from the UK*. Cambridge University Press.

Smith, J. (2024b). *AI misdiagnosis in telemedicine: Case studies from the UK*. Cambridge University Press.

Suryadi, A. (2021a). *Rule of law and digital governance in Indonesia*. Gadjah Mada University Press.

Suryadi, A. (2021b). *Rule of law and digital governance in Indonesia*. Gadjah Mada University Press.

Suryaprawira, T., Rahman, F., & Putri, D. (2024). Liability ambiguities in telemedicine. *Journal of Medical Ethics and Law*, *9*(1), 78–95.

Tanagho, E. A. (2008). *Smith's General Urology*.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation. *Computer Law & Security Review*, *34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Wahyudi, A. (2023). Infrastructure disparities in rural telemedicine. *Health Technology in Developing Countries*, *5*(2), 33–47.

Widyaningrum, R., & Nugroho, H. (2020). IoT-based remote patient monitoring. *Journal of Health Informatics*, *12*(4), 210–225.