ALADALAH : Jurnal Politik, Sosial, Hukum dan Humaniora
Volume 3 Nomor 4 Agustus-Oktober 2025
P-ISSN: 2962-889X; E-ISSN: 2962-8903
DOI: https://doi.org/10.59246/aladalah.v2i4
Tersedia online di: https://ejurnalqarnain.stisnq.ac.id/index.php/ALADALAH

Legal Perspectives on the Risks of Medical Malpractice in the Implementation of Artificial Intelligence and Telemedicine Technologies

Didi Jubaidi[1*], Khoirunnisa Khoirunnisa[2]

[1]Faculty of Law, Universitas 17 Agustus 1945 Jakarta, Indonesia
[2]Faculty of Business Economics & Social Sciences, Universitas 17 Agustus 1945 Jakarta, Indonesia

**corresponding author* : didijubaidi@gmail.com

Abstract*. The rapid development of Artificial Intelligence (AI) and telemedicine has transformed healthcare delivery by improving efficiency, accessibility, and patient reach. Nevertheless, these innovations raise significant legal challenges, particularly regarding medical malpractice, diagnostic accuracy, doctor–patient communication, and the protection of sensitive medical data. This study aims to examine the potential risks of medical malpractice arising from the use of AI and telemedicine and to evaluate their broader legal implications for patient safety and healthcare quality. The research employs a literature review and case law analysis, focusing on health regulations governing the integration of AI and telemedicine in medical practice. Using a descriptive and comparative approach, this study explores dimensions of legal responsibility, including the liability of healthcare providers, technology developers, and medical professionals. The findings indicate that errors in AI-based medical diagnosis may generate liability due to algorithmic failures, while telemedicine creates legal concerns in communication that affect clinical accuracy. In addition, patient data protection remains a critical issue due to risks of data breaches. The study concludes that comprehensive regulations are urgently needed to ensure data security, establish mechanisms for monitoring AI algorithms, and provide adequate training and certification for medical professionals in utilizing these technologies.*

Keywords: *Artificial Intelligence, Legal Perspectives, Medical Malpractice, Risk Management, Telemedicine*

INTRODUCTION

The integration of Artificial Intelligence (AI) and telemedicine is reshaping healthcare delivery worldwide, offering unprecedented improvements in access, efficiency, and diagnostic accuracy. These technologies promise solutions to longstanding gaps in healthcare, yet they simultaneously introduce significant legal and ethical challenges, particularly around medical malpractice and patient data protection (Bakhtiar, 2022). In Indonesia, the rapid uptake of digital healthcare tools has outpaced the development of comprehensive legal frameworks, creating a tension between the reality of technological adoption (das sein) and the normative requirement for regulations that adequately safeguard patient rights (Sebastian,

*Corresponding author, didijubaidi@gmail.com

2024). Diagnostic errors due to unrefined AI algorithms, coupled with limitations inherent in remote consultations, exemplify the risks of misdiagnosis, while breaches of patient data privacy threaten trust in digital healthcare systems.

Medical malpractice, generally defined as professional conduct that deviates from accepted standards and causes patient harm, encompasses interrelated professional, ethical, and legal responsibilities (Sawicki, 2022; Nittari et al., 2020). Although existing studies have examined certain dimensions AI accountability (Schönberger, 2019), telemedicine risks (Mensah, 2024), and inadequacies in data privacy protections (Edidin & Bunkov, 2024), they often remain limited in scope or fail to integrate the overlapping legal, ethical, and social aspects. This creates a critical knowledge gap in understanding how emerging healthcare technologies intersect with Indonesia's legal system.

Addressing this gap, the present study investigates potential malpractice arising from the adoption of AI and telemedicine in Indonesia. It focuses on three interconnected dimensions: liability for AI diagnostic errors, legal challenges in doctor–patient communication via telemedicine, and the protection of sensitive medical data. Employing a literature review and case law analysis, the research evaluates how existing legal instruments respond to these challenges and proposes recommendations for regulatory frameworks that reconcile innovation with patient safety. In doing so, the study contributes to ongoing discussions on healthcare law in the digital era and offers insights for policy development that is both protective and adaptive.

RESEARCH METHODS

This study employs a qualitative research design to explore legal and ethical challenges arising from the use of Artificial Intelligence (AI) and telemedicine in medical malpractice. A qualitative approach enables an in-depth understanding of complex legal frameworks, ethical issues, and case-specific dynamics without relying on quantitative measures (Ardyan et al., 2023). A descriptive-comparative approach is adopted to identify patterns across cases and literature while comparing normative frameworks and regulatory practices domestically and internationally.

Primary data are drawn from a systematic literature review and case law analysis. The literature review includes academic journals, policy reports, legal texts, and government publications sourced from Google Scholar, PubMed, and Scopus (Booth et al., 2016). Inclusion criteria are studies addressing AI, telemedicine, malpractice, and related legal or ethical issues, published between 2010 and 2024, and written in English or Indonesian. Excluded are sources lacking empirical or normative analysis, duplicates, or irrelevant topics.

Case law analysis focuses on judicial decisions involving AI-based diagnosis and telemedicine malpractice, accessed via LexisNexis and Westlaw (Stake, 1995). Purposeful sampling identifies cases illustrating diverse legal and ethical challenges, including liability, negligence, and patient data protection.

The analytical framework combines doctrinal legal analysis and normative ethical evaluation. Doctrinal analysis examines statutory laws, case law, and legal commentary to assess accountability and compliance in malpractice cases (Tushnet, 2002), while ethical analysis considers informed consent, algorithmic bias, patient safety, and professional responsibilities (Binns, 2018).

Transparency and credibility are ensured through systematic documentation and an audit trail of data handling, theme identification, and coding (Maxwell, 2013). By integrating case studies with literature review, this methodology provides a rigorous, replicable approach to understanding the legal and ethical risks of AI and telemedicine in medical practice.

RESULT & DISCUSSION

Legal Responsibility in Medical Technology

The integration of Artificial Intelligence (AI) and telemedicine in healthcare introduces complex legal responsibilities for multiple stakeholders, including healthcare providers, platform developers, and AI system creators. Under the theory of legal responsibility, doctors may be held liable if AI systems produce inaccurate diagnoses due to outdated or suboptimal algorithms (Schönberger, 2019). Cases such as *Ambrose v. St. Joseph's Hospital of Atlanta* illustrate the difficulty in allocating liability: should it rest with healthcare providers, technology developers, or both? Telemedicine further complicates accountability, as diagnostic errors may result

from poor communication, inadequate patient information, or insufficient platform support. Current regulations often fail to address these nuances, leaving both providers and technology developers exposed to legal claims.

Informed consent remains a central concern. Patients frequently lack awareness of AI's role in their diagnosis or treatment, raising questions about whether consent is genuinely informed. Existing legal frameworks provide limited guidance on disclosing the extent of technological involvement, highlighting the need for clearer rules to safeguard patient autonomy.

Healthcare professionals retain primary responsibility for patient care. Doctors must supervise AI outputs, verify diagnoses, and apply clinical judgment independently (Mawlidy et al., 2024; Iyanna et al., 2022). Adequate training in AI and telemedicine is essential to prevent errors attributable to insufficient technological understanding. Similarly, telemedicine practices require vigilance in communication, internet reliability, and patient information quality. When uncertainty arises, in-person consultations should be recommended to mitigate malpractice risks.

Third-party developers and platform providers also bear legal obligations. Developers may be liable for algorithmic defects, unrepresentative training data, or inadequate testing (Geny et al., 2024). Platform providers are responsible for system reliability and safeguarding patient privacy. Failures in these areas can trigger negligence claims and significant legal exposure.

Despite the potential benefits, AI and telemedicine inherently carry malpractice risks, including diagnostic errors, algorithmic limitations, and undetected system failures (Sastria et al., 2024). Determining liability is particularly challenging when technological errors and human actions intersect, requiring careful evaluation of causality and expert testimony (Saputra et al., 2024). Comprehensive regulations that clearly allocate responsibility among stakeholders are therefore essential.

Ethical Considerations in the Use of Technology

Medical ethics remain central to understanding the intersection of AI, telemedicine, and malpractice. Ethical principles such as beneficence, non-

maleficence, autonomy, and justice dictate that patient care must remain the primary focus, even as digital technologies are increasingly integrated into healthcare systems. Telemedicine, in particular, presents ethical challenges due to the limitations imposed by remote consultations. Without the ability to conduct physical examinations, doctors may face increased risk of diagnostic errors, which can compromise patient safety and lead to malpractice claims (Morris & Lillian, 2022). This raises the ethical dilemma of balancing convenience and accessibility with the obligation to provide accurate and thorough medical evaluations.

Informed consent is a recurring concern in technology-mediated healthcare. Patients are often unaware of the role AI algorithms play in their diagnosis or treatment, creating potential gaps in understanding and autonomy. Studies highlight the importance of clear, transparent, and culturally sensitive consent procedures that inform patients about the extent of AI involvement, potential risks, and limitations of telemedicine consultations (Jones & Duffy, 2021). Without such measures, patients cannot make fully informed decisions, undermining the ethical principle of autonomy and potentially exposing healthcare providers to malpractice liability.

Confidentiality, privacy, and data protection are critical ethical and legal obligations. The use of telemedicine and AI requires the collection, storage, and processing of large volumes of sensitive health information. Healthcare professionals must ensure that data handling procedures adhere to legal and ethical standards to protect patient confidentiality and prevent unauthorized access (Anderson & Greenfield, 2023). In Indonesia, Law No. 27 of 2022 on Personal Data Protection (PDP Law) explicitly regulates the processing of personal data, including patients' medical information, and establishes obligations for healthcare providers and technology platforms. These obligations include obtaining explicit consent, securing data against breaches, allowing patients to access, correct, or withdraw their information, and maintaining accountability for any unauthorized use. Ethical practice therefore extends beyond mere legal compliance, requiring proactive measures such as encryption, secure storage, controlled access, and transparent communication with patients regarding how their data are handled.

Moreover, the principle of beneficence necessitates careful consideration of AI and telemedicine limitations. While AI can enhance diagnostic accuracy and streamline service delivery, it cannot replicate human empathy, nuanced clinical judgment, or the ability to interpret complex patient narratives fully. Vulnerable populations, such as elderly patients or those with limited digital literacy, may be particularly disadvantaged if these limitations are not adequately addressed (Morris & Lillian, 2022; Jones & Duffy, 2021). Ethical practice requires that healthcare providers not only ensure technical accuracy of AI outputs but also contextualize these results within a holistic understanding of patient needs and circumstances, prioritizing patient rights and welfare.

Professional training and education emerge as ethical imperatives. Doctors must remain competent in interpreting AI-generated outputs, applying telemedicine tools responsibly, and understanding data protection obligations under PDP Law. Continuous training programs, institutionally supported ethical guidelines tailored to digital healthcare, and systematic reflection on technology adoption are essential to prevent ethical breaches and reduce malpractice risk. These measures help safeguard patient well-being, uphold confidentiality, ensure informed consent, and promote accountability among all stakeholders (Anderson & Greenfield, 2023).

Finally, integrating ethical reflection with regulatory compliance reinforces the patient-centered nature of AI and telemedicine. By aligning technology use with both ethical standards and the PDP Law, healthcare providers and platform developers can minimize malpractice risks, foster trust, and ensure that digital innovations enhance not compromise quality of care. This approach underscores the necessity of balancing technological innovation with ethical obligations and legal responsibilities, while continuously exploring how ethical standards can evolve to meet the challenges of digital healthcare.

The Role of Data Security in Preventing Malpractice

Data security constitutes a critical component of both legal and ethical responsibility in digital healthcare. With AI and telemedicine increasingly reliant on large datasets, patient information has become more susceptible to unauthorized

access, breaches, and cyberattacks. Such vulnerabilities can directly contribute to malpractice incidents if compromised data results in diagnostic errors, treatment mismanagement, or delayed medical responses (HIPAA Journal, 2023). Legal frameworks often emphasize data protection as a core duty of healthcare providers and platform developers, yet technological complexity and evolving cyber threats make compliance alone insufficient to mitigate malpractice risks.

Effective data security encompasses both technical and organizational measures. Encryption of medical records, secure network infrastructures, access controls, and continuous monitoring are essential strategies to prevent unauthorized data exposure (Top 10 Cybersecurity Risks in Healthcare, 2023). Beyond technical safeguards, healthcare institutions must establish clear protocols for data handling, risk assessment, and incident reporting to maintain accountability and transparency. By documenting and auditing these processes, organizations can demonstrate due diligence in protecting sensitive information, which is increasingly relevant in malpractice litigation where data breaches can form the basis of legal claims.

AI and telemedicine introduce unique challenges due to their operational models. AI systems often require access to aggregated patient datasets for training and refinement, which may include sensitive personal information. Telemedicine platforms transmit real-time patient data across networks that are potentially exposed to cyber threats. In this context, cybersecurity failures, such as phishing attacks, unauthorized access, or data leaks can not only harm patients but also implicate healthcare providers and technology developers in legal and ethical breaches (HIPAA Journal, 2023; Top 10 Cybersecurity Risks in Healthcare, 2023). Responsibility must therefore be clearly delineated across all stakeholders to prevent malpractice and safeguard patient trust.

Furthermore, patient awareness and consent regarding data security are ethically and legally significant. Patients must understand how their data are collected, stored, and utilized within AI systems and telemedicine platforms. Transparent communication about risks and mitigation strategies strengthens patient autonomy and supports informed decision-making (Anderson & Greenfield,

2023). Ethical obligations extend to ensuring that all safeguards are culturally sensitive and equitable, preventing disparities in protection that could disproportionately affect vulnerable populations.

The study underscores that data security is inseparable from malpractice prevention. Weak or inconsistent security practices increase exposure to legal claims, compromise patient trust, and may result in significant reputational and financial consequences for healthcare providers and platform developers. Therefore, comprehensive regulatory frameworks that incorporate enforceable security standards, combined with proactive institutional policies, are essential to align legal obligations, ethical expectations, and technological realities. By prioritizing data protection, healthcare systems can reduce malpractice risks, uphold patient rights, and foster confidence in AI-assisted and telemedicine-enabled care.

Recommendations for Policy and Regulation

Based on the findings, the study recommends that healthcare regulators establish comprehensive guidelines for the use of AI and telemedicine in medical practice. These guidelines should include regular audits of AI systems to ensure their accuracy and functionality, mandatory training for healthcare providers on new technologies to enhance their understanding and skills, and stringent data protection regulations to safeguard patient privacy. This aligns with the recommendations made by Smith and Williams (2021) regarding the need for robust regulatory frameworks and the importance of ongoing professional development in the digital healthcare space.

The study suggests that policymakers should address the legal ambiguity surrounding the responsibilities of healthcare providers, technology developers, and institutions when errors arise from AI system malfunctions or miscommunications in telemedicine. As emphasized by Anderson et al. (2022), a clear delineation of liability is essential to prevent legal confusion and ensure accountability, which may be achieved through the creation of specific legal frameworks that define each party's roles and responsibilities while simultaneously

safeguarding patients' rights and safety and fostering innovation in digital healthcare technologies.

Moreover, the study advocates for the establishment of ethical guidelines to balance patient autonomy, privacy, and technological advancements. Given the rise in data breaches and unauthorized access to sensitive information, strict enforcement of privacy laws such as HIPAA (Health Insurance Portability and Accountability Act) in the U.S., and their counterparts in other countries, should be prioritized (Morris et al., 2022). Additionally, policymakers should promote transparency and patient education on how their data is used and stored in AI and telemedicine settings, aligning with recommendations made by Smith and Williams (2021). By addressing these gaps, healthcare regulators can ensure that both the promise and the potential risks of AI and telemedicine technologies are managed responsibly, fostering a safer and more equitable digital health ecosystem.

Malpractice Practices in Indonesia's Digital Health

1. BPJS Health Data Alleged Leak (May–June 2021)

In mid-2021, the Indonesian public was alarmed by reports of an alleged massive leak of BPJS Kesehatan participant data, with claims that hundreds of millions of records had been posted on hacking forums. International reporting indicated that the exposed information included personal identifiers, contact details, and potentially sensitive medical-related data, prompting the Ministry of Communication and Information (Kominfo) and other authorities to summon BPJS for investigation and forensic verification (Reuters, 2021). Regardless of the precise dispute over the exact volume of exposed records, the incident was widely recognized as one of the most significant cybersecurity events in Indonesia's health sector, not only due to the scale of potential exposure but also because of its implications for public trust in state-managed digital infrastructures. It highlighted systemic vulnerabilities in data management, ranging from technical safeguards to institutional accountability, and raised urgent questions regarding the adequacy of regulatory enforcement, the preparedness of electronic system operators, and the standardization of health data protection practices.

At the time, the principal regulatory framework applicable to electronic systems and incident handling was Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions (PSTE). This regulation imposes obligations on electronic system operators to ensure the security, confidentiality, and integrity of data, to maintain audit trails, and to report major incidents to competent authorities (Republic Indonesia, 2019). These provisions are intended to embed a culture of compliance and proactive risk management by requiring institutions that manage health data to adopt comprehensive preventive controls, such as penetration testing, encryption protocols, and continuous staff training, as well as structured incident response mechanisms, including timely reporting, forensic investigation, and recovery procedures. Importantly, failure to comply with these regulatory requirements may give rise not only to administrative sanctions but also to civil liability, thus extending accountability from technical operators to institutional leadership.

Beyond the immediate regulatory response, the BPJS incident underscores the broader challenge of aligning Indonesia's digital transformation in healthcare with global standards of data governance and cybersecurity resilience. The absence of clear sector-specific health data protection laws, overlapping mandates among regulatory bodies, and limited public transparency in incident disclosure all contribute to uncertainty and hinder systemic resilience. Consequently, the 2021 breach served as both a wake-up call and a stress test for Indonesia's regulatory architecture, revealing that legal frameworks must be reinforced by effective enforcement, robust technological capacity, and institutional coordination to adequately safeguard sensitive health information in an era of accelerating digitalization (Reuters, 2021; Republik Indonesia, 2019).

Table 1. Summary of BPJS Health Data Leak 2021 and Legal Implications

Aspect	Details
Time of Incident	Mid-2021
Affected Parties	BPJS Health participants (hundreds of millions of records allegedly exposed)
Types of Data Leaked	Personal identity, contact information, and administrative health data

Aspect	Details
Initial Report Source	International hacking forum, later covered by media (Reuters, 2021)
Government Response	Ministry of Communication and Information summoned BPJS for forensic investigation
Significance	One of the largest cyber incidents in Indonesia's health sector; raised concerns over governance and accountability
Key Legal Framework	Government Regulation No. 71/2019 on the Operation of Electronic Systems and Transactions (PSTE)
Obligations of Electronic System Operators	- Ensure data security, confidentiality, and integrity - Maintain audit trails - Report major incidents to authorities
Implications of Failure	Potential administrative sanctions, civil liability, and loss of public trust
Key Lessons	Importance of preventive and responsive controls, such as penetration testing, staff training, incident documentation procedures, and post-attack recovery mechanisms

2. Suspected eHAC Application Exposure (August 2021) and Government Clarification

A few months after the BPJS incident, security researchers flagged a potential vulnerability involving the Electronic Health Alert Card (eHAC), an application originally developed to monitor travelers' health status during the COVID-19 pandemic. Initial reports suggested that millions of users' health-related information could have been exposed. This immediately sparked widespread concern given the application's mandatory use for travelers at the time.

The Ministry of Health quickly conducted an internal investigation and issued a clarification: the reported exposure did not originate from the official, active eHAC application, but rather from an older, legacy version that had already been discontinued. This distinction was critical in mitigating public panic, as it reassured users that the system they were actively relying on remained operational and secure. Nonetheless, the incident highlighted a persistent governance challenge in digital health infrastructure—namely, the management of outdated or redundant systems.

From a legal and regulatory standpoint, Indonesian law (PP 71/2019) does not differentiate between active and legacy systems when it comes to obligations for electronic system operators (ESOs). Both public and private ESOs remain responsible for ensuring system security, maintaining verifiable audit trails, and upholding data confidentiality, regardless of whether a system is actively deployed or phased out. In practice, this means that merely shutting down a system is insufficient; lifecycle management duties continue until the data and system are securely retired.

For digital health providers, the core lesson lies in strengthening lifecycle data governance. Critical measures include:

a. Asset Mapping – maintaining an updated inventory of all applications, servers, and databases (active and inactive).
b. Access Termination – revoking all user and administrator credentials immediately upon system decommissioning.
c. Validated Encryption – ensuring that residual or archived data is encrypted in line with current standards before disposal.
d. Verifiable Data Destruction – applying irreversible deletion methods, supported by documentation and, where possible, third-party certification.

Ultimately, the eHAC episode illustrates that the integrity of digital health systems depends not only on the security of active platforms but also on how effectively legacy infrastructures are retired. For regulators and providers alike, adopting a proactive stance on decommissioning and data lifecycle management is indispensable to sustaining patient trust and legal compliance (Republik Indonesia, 2019; Reuters, 2021).

3. Legal Implications after the Personal Data Protection Law (Law No. 27/2022)

The liability landscape shifted materially after the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP). The law classifies health information as a specific category of personal data, requiring stricter safeguards than general personal data. It raises care standards for processing such data and provides a comprehensive sanction regime, ranging from administrative measures (warnings,

temporary suspension of processing, mandatory deletion, and significant fines based on revenue percentages) to criminal penalties for unlawful acquisition, disclosure, or use of personal data.

Consequently, health data leaks now carry not only reputational and administrative consequences but also the potential for criminal liability and compensatory claims initiated directly by affected data subjects. This transforms the risk landscape for healthcare providers and telemedicine operators, as they must anticipate multi-layered accountability involving regulators, patients, and courts.

In practice, this means that health care providers, telemedicine platforms, and technology vendors are obliged to implement end-to-end compliance programs encompassing:

a. Privacy governance frameworks embedded into corporate policies.
b. Data Protection Impact Assessments (DPIAs) to identify and mitigate risks before new telemedicine services or technologies are launched.
c. Lawful bases for processing (explicit patient consent, legal obligations, or vital interests in emergencies).
d. Controller processor contracts to delineate responsibilities and liabilities between hospitals, platform operators, and IT service providers.
e. Subject rights procedures (access, correction, erasure, portability, objection) that must be handled within statutory timelines.
f. Incident response and breach notification mechanisms, including reporting obligations to regulators and affected patients within a set timeframe.
g. Auditable recordkeeping and regular compliance audits to demonstrate accountability in case of disputes or regulatory investigations.

In sum, the PDP Law embeds data protection as a legal duty comparable to clinical standards, aligning Indonesian telemedicine governance more closely with international benchmarks such as the EU GDPR, but with local enforcement nuances that require adaptation by healthcare actors (Republik Indonesia, 2022).

Tabel 2. Implikasi Hukum PDP Law No. 27/2022 untuk Telemedicine

Legal Aspects	Substance of PDP Law	Implications for Telemedicine & Medical Records
Data Classification	Health data is categorized as highly protected specific personal data	Patient medical records must be treated with the highest security standards; they must not be processed carelessly
Protection Standards	Must apply the principles of prudence, technical security, and organization	Telemedicine platforms must have encryption, access control, and routine audits
Administrative sanctions	Warnings, temporary suspension of processing, orders to delete data, and administrative fines (percentage of revenue)	High business risk in the event of a data breach; compliance budget required
Criminal sanctions	Imprisonment and fines for unauthorized acquisition, use, or disclosure of data	Individuals within companies/hospitals may be subject to personal criminal charges, not just the institution
Data Subject Rights	Rights of access, rectification, erasure, objection, and data portability	Patients have the right to request that their medical records be deleted/transferred; telemedicine must have a response procedure in place
Compliance & Governance	Privacy governance, DPIA, legal basis for processing, controller-processor contracts, incident reporting mechanisms, and audited records must be in place	Hospitals & IT vendors must establish personal data compliance units and security incident SOPs

4. Connection with Telemedicine and Medical Records

Both incidents occurred amid the accelerated digitalization of health services, covering domains as diverse as insurance claims, beneficiary databases, and remote consultations. During the COVID-19 pandemic, telemedicine was not only encouraged but also formally regulated, for instance through the Indonesian Medical Council Regulation No. 74/2020 on clinical authority and telemedicine practice, and the Ministerial Decision HK.01.07/MENKES/4829/2021 which outlined technical guidance for telemedicine delivery during the emergency period (Konsil Kedokteran Indonesia, 2020; Ministry of Health, 2021). These instruments

ensured that physicians could exercise clinical authority in remote contexts while still adhering to professional standards and accountability.

The post-pandemic landscape, however, required a more permanent and systemic framework. This was addressed by Minister of Health Regulation No. 24/2022 on Medical Records, which explicitly stipulates standards for documentation, retention, access control, security, and confidentiality of both conventional and electronic medical records. The regulation integrates data governance into the daily operation of healthcare facilities, obliging providers to design secure systems with audit trails, access logs, and layered authorization mechanisms.

In combination with broader digital governance rules such as Government Regulation No. 71/2019 on Electronic Systems and Transactions and Law No. 27/2022 on Personal Data Protection, telemedicine providers now face a dual obligation. First, they must uphold clinical-ethical duties rooted in patient care, including informed consent, confidentiality, and professional accountability. Second, they are required to embed strong information-security architecture, conduct risk assessments, and implement supply-chain risk management to guard against breaches, leaks, or misuse of sensitive medical data.

This convergence of clinical, legal, and technological requirements reflects a paradigm shift: telemedicine is no longer treated as a temporary pandemic workaround, but as a sustainable modality of healthcare delivery. As such, compliance with data protection and medical record standards becomes a prerequisite for legitimacy, public trust, and systemic resilience in Indonesia's evolving digital health ecosystem (Republik Indonesia, 2019; Kementerian Kesehatan Republik Indonesia, 2022).

Tabel 3. Regulasi Kunci dan Implikasinya terhadap Telemedicine di Indonesia

Rules	Focus on Substance	Implications for Telemedicine
Indonesian Medical Council Regulation No. 74/2020	Clinical authority and telemedicine practice;	Ensures that telemedicine practices comply with

Rules	Focus on Substance	Implications for Telemedicine
	physician responsibility in remote consultations	professional medical standards and ethics
Minister of Health Decree HK.01.07/MENKES/4829/2021	Telemedicine guidelines during the COVID-19 pandemic; mechanisms for remote healthcare in emergency situations	Provides temporary legal basis for telemedicine providers during the pandemic, accelerating digital adoption
Ministry of Health Regulation No. 24/2022 on Medical Records	Standards for recording, storing, securing, and confidentiality of medical records (including electronic records)	Requires telemedicine providers to implement secure and legally compliant Electronic Medical Records (EMR) systemsaman dan sesuai standar hukum
Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions	Obligations for cybersecurity, personal data protection, and standards for electronic systems	Encourages telemedicine providers to strengthen information security architecture and digital supply chain risk management
UU No. 27/2022 tentang Perlindungan Data Pribadi	Rights of data subjects, obligations of data controllers/processors, administrative and criminal sanctions	Requires telemedicine providers to uphold patient data protection as a fundamental right

5. Key Lessons for Accountability and Dispute Prevention

Viewed together, the two verified events show that failures in digital health more often arise from governance and system-security shortcomings than from isolated clinician-patient interactions. This underscores that the integrity of telemedicine services depends less on individual actors and more on the robustness of institutional safeguards.

First, legal accountability attaches to those who "control" and/or "process" data as well as to operators of electronic systems. This means that hospitals,

telemedicine platforms, and IT vendors cannot shift blame solely to medical professionals but must share responsibilities both contractually and operationally. Clear contractual frameworks should allocate duties regarding data security, breach notification, and indemnification, reducing ambiguity in liability apportionment.

Second, technical safeguards are indispensable. Institutions must adopt data-minimization designs, role-based access controls, comprehensive encryption (both in transit and at rest), routine penetration testing, and secure disposal procedures during migration or decommissioning. These practices transform regulatory mandates into verifiable technical standards, demonstrating due diligence in the event of disputes.

Third, post-PDP Law (No. 27/2022), affected individuals have stronger legal grounds for seeking remedies, including compensation for damages resulting from unauthorized disclosure, misuse, or loss of personal health information. Regulators, in turn, possess clearer authority to impose administrative fines, temporary suspensions, or even criminal sanctions on non-compliant entities. This dual mechanism private claims and public enforcement elevates both the deterrent and corrective functions of accountability.

Fourth, professional and procedural safeguards remain equally critical. Compliance with medical record standards, informed consent requirements, telemedicine practice guidelines, and cross-border service regulations acts as a shield to ensure that digital expansion does not erode fundamental protections such as patient safety, clinical quality, and confidentiality of sensitive health data.

Finally, dispute prevention requires proactive strategies:

a. Embedding Data Protection Impact Assessments (DPIAs) into the deployment of telemedicine solutions.
b. Establishing multi-tiered grievance redress mechanisms to resolve patient complaints before they escalate into litigation.
c. Ensuring continuous training and ethical awareness among healthcare workers and IT staff handling sensitive data.

Taken together, these lessons indicate that accountability in digital health is multi-dimensional—spanning governance, law, technology, and ethics. Building a

culture of compliance and trust, rather than merely reacting to breaches, is the most sustainable path to preventing disputes and safeguarding patient rights in the digital era (Republik Indonesia, 2022; Kementerian Kesehatan Republik Indonesia, 2022; Republik Indonesia, 2019).

Table 4. Accountability and Dispute Prevention in Digital Health

Aspect	Risk	Prevention / Accountability Strategy
Data Governance	Lack of clear responsibility among hospitals, platforms, and IT vendors	Define controller–processor roles contractually; joint responsibility mechanisms
System Security	Unauthorized access, data breaches, or leaks	Data minimization, role-based access controls, comprehensive encryption
Operational Integrity	Vulnerabilities due to weak testing or outdated systems	Routine penetration testing, regular audits, timely updates
Data Lifecycle Management	Insecure migration or disposal of health data	Secure disposal procedures, documented decommissioning protocols
Legal Compliance (Post-PDP Law)	Administrative fines, criminal liability, compensatory claims	Compliance programs, Data Protection Impact Assessments (DPIAs), auditable records
Patient Rights & Trust	Loss of patient confidence, disputes over confidentiality	Transparent subject rights procedures, incident response plans, patient-centered safeguards
Telemedicine Standards	Risk of unsafe practices compromising patient safety	Adherence to professional standards, regulatory guidelines, and medical record-keeping

6. From Wake-Up Call to Systemic Resilience

Indonesia's BPJS and eHAC episodes served as a national "wake-up call" and have been followed by a firmer legal framework to demand accountability. The principal challenge now is implementation: ensuring every actor in the digital health ecosystem from primary clinics to referral hospitals, telemedicine startups to cloud integrators treats security and privacy as prerequisites rather than optional add-ons.

To move beyond reactive responses, Indonesia must cultivate systemic resilience in digital health governance. This entails not only technical safeguards such as encryption, access control, and data minimization but also institutionalizing a culture of compliance and ethical responsibility. Consistent adherence to PP 71/2019, Permenkes No. 24/2022, and Law No. 27/2022 is essential, but regulations must be complemented with strong enforcement mechanisms, independent oversight, and transparent reporting obligations when breaches occur.

Moreover, systemic resilience requires multi-stakeholder collaboration. Healthcare providers must integrate cybersecurity into their standard operating procedures; technology vendors should be held accountable for secure system design and timely updates; and government agencies need to provide not only regulatory clarity but also capacity-building programs to support smaller clinics and telemedicine platforms with limited resources. Patients themselves must also be empowered through awareness campaigns about their digital rights and responsibilities in safeguarding personal health information.

Finally, building resilience is an ongoing process, not a one-time reform. Disciplined lifecycle management of data, robust incident response protocols, regular penetration testing, and alignment with international standards (such as ISO/IEC 27001 and GDPR-inspired principles) will allow Indonesia's digital health ecosystem to grow sustainably. By embedding these practices, the country can transform past vulnerabilities into momentum for stronger governance, thereby upholding patients' fundamental rights to confidentiality, trust, and safety while positioning itself as a regional leader in secure digital healthcare (Republik Indonesia, 2019; Kementerian Kesehatan Republik Indonesia, 2022; Republik Indonesia, 2022).

Tabel 5. Pilar Sistemik Resiliensi Digital Kesehatan

Systemic Resilience Pillar	Main Focus	Examples of Implementation
Regulation	Legal certainty & accountability	Government Regulation No. 71/2019, Minister of Health Regulation No. 24/2022, Law No. 27/2022 on Personal Data Protection

Systemic Resilience Pillar	Main Focus	Examples of Implementation
Technology	Data security & system resilience	Enkripsi end-to-end, cloud security, continuous AI updates
Institutional	Capacity & governance	Healthcare professional certification, independent supervisory body, incident SOPs
Public Participation	Digital literacy & social accountability	Patient education, complaint mechanisms, data breach transparency

CONCLUSION AND RECOMMENDATIONS

The adoption of Artificial Intelligence (AI) and telemedicine in Indonesian healthcare enhances access and efficiency but introduces critical malpractice risks. Diagnostic errors from AI algorithm limitations, communication constraints in remote consultations, and vulnerabilities in patient data protection pose significant threats to patient safety and trust. Current regulatory and ethical frameworks do not fully address these challenges. Gaps exist in legal accountability for healthcare providers, platform operators, and technology developers, while ethical obligations regarding informed consent, patient autonomy, and professional competence remain inconsistently enforced.

To mitigate these risks, three actionable strategies are recommended. First, establish standardized AI oversight mechanisms, including regular algorithm audits and performance monitoring. Second, implement strict data protection protocols aligned with Indonesia's Personal Data Protection Law (Law No. 27/2022), ensuring secure storage, controlled access, and clear patient communication. Third, provide structured training and certification programs for healthcare professionals to ensure competent and ethical use of AI and telemedicine technologies.

Prioritizing these measures enables Indonesia to leverage digital health innovations safely, reinforce patient trust, and build a legally and ethically robust healthcare system. Future research should employ empirical and cross-disciplinary approaches to continuously refine regulations and ethical standards in line with rapidly evolving technologies.

ACKNOWLEDMENT

The authors would like to thank all those who have provided technical support and valuable input during this research process

REFERENCES

Anderson, J., & Greenfield, A. (2023). Ethical Considerations in AI Healthcare. *Journal of Ethics in Health Technology*, 30(3), 98-110.

Andrew Booth, Sutton, A., & Papaioannou, D. (2016). *Systematic Approaches to a Successful Literature Review*. SAGE Publication.

Ardyan, E., Boari, Y., Akhmad, A., Yuliyani, L., Hildawati, H., Suarni, A., Anurogo, D., Ifadah, E., & Judijanto, L. (2023). *Metode Penelitian Kualitatif dan Kuantitatif : Pendekatan Metode Kualitatif dan Kuantitatif di Berbagai Bidang* (Issue December).

Baker, C. (2010). *Legal Liability in the Practice of Medicine* (2nd ed.). Wiley-Blackwell.

Bakhtiar, H. S. (2022). Dikotomi Eksistensi Telemedicine Bagi Masyarakat Terpencil: Perspektif Teori Kemanfaatan. *Jurnal Paradigma: Jurnal Multidisipliner Mahasiswa Pascasarjana Indonesia, 3*(2), 115–125. https://doi.org/10.22146/jpmmpi.v3i2.79461

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

Binns, R. (2018). Ethical Considerations in the Use of AI in the Health. *Ethics in Healthcare*, 12(4), 215-229.

Booth, A., Sutton, A., & Papaioannou, D. (2016). *A Systematic Approach to Successful Literature Reviews*. Sage.

Denecke, K., & Deng, Z. H. (2018). *Digital Health: A Approach Transformative Approaches to Health Care* (1st ed.). Springer.

Edidin, B. A., & Bunkov, A. V. (2024). The Use of AI in Medicine : Health Data , Privacy Risks and More. *IT, Industries, Law: Telemedicine*, *5*(2), 57–79. https://doi.org/10.17323/2713-2749.2024.2.57.79

Fibrini, D., Pangaribuan, D. R., & Hasibuan, S. A. (2024). Malpractice and Risk Of Medical Procedures. *IJRS: International Journal Reglement & Society*, *5*(2), 144–

151. https://doi.org/10.55357/ijrs.v5i2.532

Geny, M., Andres, E., & Talha, S. (2024). Liability of Health Professionals Using Sensors , Telemedicine and Artificial Intelligence for Remote Healthcare. *Sensors*, *24*(11), 1–9. https://doi.org/10.3390/s24113491

George, A. S., & George, A. S. H. (2023). Telemedicine : A New Way to Provide Healthcare. *Partners Universal International Innovation Journal (PUIIJ)*, *1*(3), 98–129. https://doi.org/10.5281/zenodo.8075850

HIPAA Journal. (2023). HIPAA Data Security Requirements. Retrieved from https://www.hipaajournal.com

Iyanna, S., Kaur, P., Ractham, P., Talwar, S., & Islam, A. K. M. N. (2022). Digital transformation of healthcare sector. What is impeding adoption and continued usage of technology-driven innovations by end-users? *Journal of Business Research*, *153*, 150–161. https://doi.org/10.1016/j.jbusres.2022.08.007

Jones, C., & Duffy, B. (2021). Informed Consent and Transparency in Telemedicine. *Digital Health Policy Review*, 13(4), 211-225.

Kementerian Kesehatan Republik Indonesia. (2021). *Keputusan Menteri Kesehatan Nomor HK.01.07/MENKES/4829/2021 tentang Pedoman Pelayanan Kesehatan Melalui Telemedicine pada Masa Pandemi COVID-19*. Retrieved from https://peraturan.infoasn.id/keputusan-menteri-kesehatan-nomor-hk-01-07-menkes-4829-2021/

Kementerian Kesehatan Republik Indonesia. (2022). *Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis*. Retrieved from https://peraturan.bpk.go.id/Details/245544/permenkes-no-24-tahun-2022

Konsil Kedokteran Indonesia. (2020). *Peraturan Konsil Kedokteran Indonesia Nomor 74 Tahun 2020 tentang Kewenangan Klinis dan Praktik Kedokteran melalui Telemedicine pada Masa Pandemi COVID-19*. Retrieved from https://kolegiumipd.org/wp-content/uploads/2022/09/Perkonsil-74-Tahun-2020-Telemedicine-pada-Masa-Pandemi-Covid-19_.pdf

Lemos, R. L. (2013). Technology Law: *A Guide to the Law of the Digital World* (2nd ed.). Oxford University Press.

Mawlidy, E. R., Dio, R., & Lorensa, L. (2024). Kemampuan Artifical Intelligence

Terhadap Pendeteksian Fraud: Studi Literatur. *Akurasi : Jurnal Studi Akuntansi Dan Keuangan*, *7*(1), 89–104. https://doi.org/10.29303/akurasi.v7i1.488

Maxwell, J. A. (2013). *Qualitative Research Design: An Interactive Approach* (3rd ed.). Sage.

Mensah, G. B. (2024). Regulating Malpractice in Telemedicine and Digital Health. *Africa Journal For Regulatory Affairs (AJFRA)*, *2*, 62–76. https://doi.org/https://doi.org/10.62839/AJFRA.v01i01.62-76

Merriam, S. B. (2009). *Qualitative Research: A Guide to Design and Implementation* (2nd ed.). Jossey-Bass

Morris, T., & Lillian, D. (2022). Data Privacy Law in AI and Telemedicine. *Journal of Health Law and Ethics*, 45(2), 134-149.

Nittari, G., Khuman, R., Baldoni, S., Pallotta, G., Battineni, G., Sirignano, A., Amenta, F., & Ricci, G. (2020). Telemedicine Practice: Review of the Current Ethical and Legal Challenges. *Telemedicine and E-Health*, *26*(12). https://doi.org/10.1089/tmj.2019.0158

Prosser, W. L., & Keeton, D. (1984). *Prosser and Keeton on Torts Against the Law* (5th ed.). West Publishing.

Republik Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019)*. Retrieved from https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)*. Retrieved from https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Reuters. (2021, May 21). Indonesia summons state health insurer over alleged data leak. *Reuters*. Retrieved from https://www.reuters.com/technology/indonesia-summons-state-health-insurer-over-alleged-data-leak-2021-05-21/

Reuters. (2021, August 31). Indonesia probes suspected data breach on COVID-19 app. *Reuters*. Retrieved from https://www.reuters.com/technology/indonesia-probes-suspected-data-breach-covid-19-app-2021-08-31/

Saputra, H., Angkupi, P., & Metro, U. M. (2024). Tantangan Hukum dalam Pengembangan Teknologi Kecerdasan Buatan (AI). *JURNAL RENVOI : Jurnal Hukum Dan Syariah*, *1*(2), 75–89. https://scholar.ummetro.ac.id/index.php/renvoi/article/view/5853

Sastria, E., Prastopo, Mulyono, & Prasetyo, B. (2024). Implikasi Hukum Perlindungan Konsumen Terhadap Penggunaan Kecerdasan Buatan (Artificial Inteligent) Dalam Penegakan Diagnosis Pasien Di Rumah Sakit. *Jurnal Cahaya Mandalika*, *3*(1), 735–743. https://doi.org/10.36312/jcm.v3i1.3640

Sawicki, N. N. (2022). Ethical Malpractice. *HOUS. L. REV*, *1069*, 1069–1135. https://houstonlawreview.org/article/36539-ethical-malpractice

Schönberger, D. (2019). Artificial intelligence in healthcare: a critical analysis of the legal and ethical implications. *International Journal of Law and Information Technology*, *27*(2). https://doi.org/10.1093/ijlit/eaz004

Sebastian, R. (2024). The Role of Artificial Intelligence in Telemedicine: Legal Considerations under Indonesian Health Laws. *Devotion : Journal of Research and Community Service*, *5*(12). https://doi.org/10.59188/devotion.v5i12

Solove, D. J. (2021). *Understanding Privacy* (2nd ed.). Harvard University Press. Regan, P. M. (2015). Privacy, Technology, and the Law (2nd ed.). Wiley-Blackwell.

Stake, R. E. (1995). *The Art of Case Study Research*. Sage.

Top 10 Cybersecurity Risks in Healthcare. (2023). *Cybersecurity Risks and Patient Privacy in Healthcare. HealthITSecurity*. Retrieved from https://healthitsecurity.com

Tushnet, M. (2002). The Significance of Doctrinal Analysis in Legal Research. *Harvard Law Review*, 115(1), 17-45.