International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 01-06-2025, Accepted: 02-07-2025, Published: 17-07-2025
Volume 7, Issue 3, 2025, Page No. 15-21

Assessing legal and institutional readiness for patient data protection in the age of big health data: An empirical study of health facilities in Indonesia

Rospita Adelina Siregar*, Nanin Koeswidi Astuti
Faculty of Law, The Christian University of Indonesia, Jakarta, Indonesia

Abstract
The rapid expansion of digital health systems in Indonesia has raised critical concerns regarding patient data privacy and institutional compliance with emerging legal standards. This study explores how healthcare facilities implement data protection practices within the framework of Indonesia's Personal Data Protection Law (Law No. 27/2022). Employing a qualitative methodology, data were gathered through semi-structured interviews with healthcare professionals, policymakers, and IT specialists, alongside field observations and document analysis from selected hospitals and clinics. Findings indicate that many healthcare personnel lack familiarities with legal data protection principles and tend to rely primarily on professional ethics. Patient information is often accessed using shared credentials, with limited technical safeguards in place. At the policy level, institutions generally lack standardized guidelines and internal audit mechanisms to ensure compliance. Regulatory authorities acknowledged the absence of detailed technical directives and noted inconsistent implementation across facilities.

IT systems, though functional, are rarely optimized for security. Critical safeguards—such as encryption, role-based access controls, and incident reporting protocols—are frequently absent. Document analysis confirms that institutional policies and standard operating procedures (SOPs) rarely reference key data protection concepts such as consent, breach notification, or accountability. The lack of designated data protection officers and clearly defined roles further compounds these challenges. This study underscores the urgent need for a comprehensive governance framework that integrates legal, technical, organizational, and behavioral dimensions of data protection. Key recommendations include strengthened regulatory support, targeted capacity-building initiatives, investment in secure IT infrastructures, and the institutionalization of privacy protocols. Without holistic reforms, patient data will remain vulnerable, and healthcare institutions risk legal non-compliance in an increasingly digitized healthcare landscape.

Keywords: Patient data privacy, Legal and regulatory compliance, personal data protection law, digital health governance, healthcare data security

Introduction

The rapid development of digital health technologies and the expansion of big data usage in healthcare have revolutionized the way patient information is stored, processed, and utilized. In developing countries such as Indonesia, this digital transformation is progressing alongside legal reforms, including the enactment of the Personal Data Protection Law (UU PDP) in 2022. As healthcare facilities increasingly rely on electronic health records and hospital information systems, the protection of patient data privacy becomes a critical ethical, legal, and technical issue [1]. Big data in healthcare offers the potential to improve medical decision-making, predictive analytics, and population health management. However, it also introduces unprecedented risks to personal privacy, especially in environments with weak cybersecurity infrastructure and inadequate legal compliance mechanisms [2]. Studies show that even minor breaches in digital health systems can result in identity theft, discrimination, or loss of patient trust [3]. Therefore, ensuring that data protection policies are implemented effectively in healthcare institutions is not only a legal obligation but also essential for public health sustainability.

Indonesia's UU PDP was modeled in part after the European Union's General Data Protection Regulation (GDPR), aiming to provide a comprehensive legal framework to protect individuals' personal data [4]. However, the healthcare sector faces unique challenges in implementing such legal standards. Many health facilities, especially outside major cities, lack the technical expertise, infrastructure, and policy mechanisms necessary to comply with national regulations [5]. This raises concerns about whether the law's adoption can genuinely strengthen the protection of sensitive medical information. In addition to legal challenges, institutional readiness plays a crucial role in operationalizing data protection laws. Hospitals and clinics must develop internal policies, assign responsible officers, and build technical systems that align with the principles of privacy and security by design [6]. In reality, many facilities in Indonesia do not have designated Data Protection Officers (DPOs), and their Standard Operating Procedures (SOPs) rarely include data breach protocols or access control frameworks. This suggests that institutional governance remains a significant gap in the country's data protection efforts.

Moreover, healthcare personnel are often not equipped with adequate knowledge or training on digital ethics and data privacy. A study by Putri *et al.* (2023) revealed that less than 30% of healthcare staff in Indonesian provincial hospitals had attended training on data security or understood the implications of data privacy laws [7]. This lack of human capacity undermines even the most well-designed technological systems, as data protection also depends on users' behaviors and decision-making. Human error, ignorance, or negligence may therefore contribute to internal breaches and legal liabilities. Previous research has

emphasized that the success of data protection implementation in healthcare settings depends on a triadic interaction between legal frameworks, institutional governance, and technological infrastructure [8]. However, in countries like Indonesia, these three pillars are often disconnected. For instance, while laws may exist, enforcement is weak; while technology may be introduced, it is not secured; and while policies may be drafted, they are not internalized by institutional actors. This fragmented reality calls for a more integrated approach to securing health information.

Given this context, the present study aims to investigate how healthcare facilities in Indonesia are prepared to protect patient data within the framework of the national PDP Law. Specifically, it examines the legal awareness of healthcare professionals, the existence of institutional mechanisms such as SOPs and internal regulations, and the technological readiness of health information systems. Using a qualitative case study approach, this research captures both the structural and cultural dimensions of data protection implementation. By highlighting empirical gaps between regulation and practice, this article contributes to the broader discourse on digital health governance in developing countries. It offers insights into the systemic barriers faced by health institutions in operationalizing legal mandates, and proposes pathways for reform grounded in policy integration, capacity building, and ethical accountability. The findings are expected to inform not only Indonesian policymakers but also international scholars and practitioners interested in health law and information governance.

Literature Review

The issue of patient data protection has evolved significantly with the advancement of health technologies and the proliferation of big data in healthcare. Initially framed as a matter of professional confidentiality within the medical code of ethics, the discourse has expanded into legal and technical domains due to the digitization of health records and the reliance on integrated hospital information systems. Digital health data, including electronic health records (EHRs), biometric identifiers, and behavioral health profiles, are now recognized as highly sensitive and valuable, requiring multilayered protection mechanisms. Scholars argue that protecting such data must involve not only individual awareness but also systemic safeguards embedded in the design and governance of healthcare institutions [9].

In the legal sphere, the European Union's General Data Protection Regulation (GDPR) has established a comprehensive framework that treats health data as a special category requiring explicit consent, purpose limitation, and data minimization. The GDPR has influenced many countries, including Indonesia, which enacted its Personal Data Protection Law (UU PDP) in 2022. While UU PDP shares key principles with GDPR, such as the designation of sensitive personal data and the need for data controllers, its implementation faces numerous contextual barriers. Unlike the EU where regulatory institutions are robust and widely enforced, Indonesia is still in the early stages of developing enforcement mechanisms, institutional alignment, and sector-specific compliance strategies [10].

Research on institutional readiness has revealed that compliance with data protection laws is not solely dependent on the existence of legal frameworks, but more importantly on the preparedness of health institutions to internalize and operationalize those frameworks. According to Rumbold and Pierscionek, effective implementation requires policies, resources, infrastructure, and culture that reinforce data privacy at every level of the organization [11]. In Indonesia, however, empirical studies have shown that many hospitals and clinics lack dedicated personnel for data protection, have minimal training for staff on digital ethics, and do not integrate privacy protocols into daily operations. Moreover, institutional resistance to change, bureaucratic inertia, and resource constraints further undermine efforts to protect patient data [12].

From a governance perspective, the integration of legal mandates with technological infrastructure and institutional behavior is crucial. Studies in Southeast Asia and sub-Saharan Africa highlight that even when technical systems such as hospital information systems are installed, their effectiveness is compromised by the absence of SOPs, unclear accountability, and inconsistent leadership support [13]. Furthermore, the lack of standardized audits and monitoring mechanisms creates a compliance vacuum where health facilities operate without adequate oversight. This situation leads to what scholars refer to as "regulatory mimicry," where institutions adopt formal compliance indicators without meaningful implementation [14]. In such contexts, data breaches often go unreported, and systemic vulnerabilities persist.

Despite increasing scholarly attention to the ethics and governance of digital health, there remains a limited body of research that specifically examines the interplay between national data protection laws and institutional realities in developing countries. In Indonesia, existing literature tends to focus on normative legal analysis or technical ICT readiness, with little attention paid to how frontline health providers interpret and implement privacy obligations. This study contributes to filling that gap by providing empirical insights into the legal awareness, technological capacity, and policy frameworks within Indonesian health facilities. It offers a grounded analysis of the practical barriers that impede the realization of data protection norms, positioning itself within the global discourse on equitable and rights-based digital health governance [15].

Research Method

This study employed a qualitative case study design to explore the legal and institutional readiness of Indonesian health facilities in implementing patient data protection under the Personal Data Protection Law (UU PDP). The qualitative approach was selected to allow for in-depth exploration of stakeholder perspectives, institutional practices, and the contextual challenges surrounding data protection implementation. The case study methodology enabled the researchers to capture complex phenomena within real-life settings and to compare findings across different types of healthcare institutions.

The research was conducted in three types of health facilities located in urban and semi-urban areas of Indonesia, including one public hospital, one private hospital, and two community health clinics. These sites were selected purposively to capture a range of institutional experiences in adopting data protection measures. Participants included healthcare professionals (such as doctors, nurses, and medical record officers), policymakers

from regulatory agencies, and information technology experts. A total of 15 individuals were interviewed using purposive and snowball sampling to ensure relevant and information-rich responses. Data were collected using three primary techniques: in-depth semi-structured interviews, document analysis, and direct observation. The interviews explored participants' knowledge of data protection laws, institutional policies, challenges in implementation, and their perceptions of privacy risks. Observations were conducted to examine how health information systems were used in practice, particularly in relation to access control, data storage, and confidentiality safeguards. Institutional documents such as standard operating procedures (SOPs), internal policies, and technical manuals were also analyzed to assess alignment with the principles of the PDP Law.

The instruments used in this study included an interview guide with thematic prompts related to legal awareness, technological practices, institutional roles, and reporting mechanisms. An observation checklist was also used to examine physical and digital security practices in clinical settings. All instruments were developed based on the theoretical framework of privacy by design and institutional data governance principles, and were pilot-tested in a non-sample clinic for refinement prior to data collection.

Data were analyzed using thematic content analysis. Interview transcripts, field notes, and documents were coded using N *Vivo* software, with emergent themes categorized into domains such as legal compliance, policy infrastructure, and operational challenges. Triangulation was conducted by comparing findings across data sources and participant groups. The credibility of findings was ensured through member checking and peer debriefing with legal and health informatics experts.

Ethical approval for this study was obtained from the institutional research ethics committee. All participants provided informed consent prior to interviews, and confidentiality was strictly maintained throughout the research process. Anonymized codes were used for participants and institutions to protect their identities. The research adhered to the ethical guidelines for qualitative research in public health and complied with national regulations regarding the use of sensitive information in research.

Results

a. Interview Findings from Healthcare Professionals

Interviews were conducted with eight healthcare professionals from four healthcare facilities located in Jakarta and Bekasi, consisting of three general practitioners, four nurses, and one medical records officer. Based on the interview instrument designed to assess their understanding of patient data protection and the application of information security principles in daily practices, it was found that their legal comprehension remained very limited. Only two individuals (25%) were able to name the Personal Data Protection Law (PDP Law) explicitly, and none could explain its core principles such as the right to consent, specific purpose limitation, or data access and correction rights.

Six out of eight participants (75%) viewed patient data protection primarily as a matter of professional ethics—i.e., avoiding verbal disclosure of medical information to outsiders—rather than associating it with digital systems, login-based data access, or applicable legal provisions. When asked about the use of medical information systems, four nurses admitted to using shared accounts during shifts for efficiency. One nurse stated, “If we have to keep logging in and out, patient queues will get even longer. So we just share one account.” This indicates that information system security procedures are not yet internalized in daily operational policies.

Regarding training, five of the eight participants reported never having received any formal education or orientation regarding personal data protection or information security since joining their respective institutions. Furthermore, when asked whether there had ever been any internal communication about the technical aspects of medical record security (e.g., strong passwords, auto-logout, or data sensitivity classification), none could recall such discussions. None of the participants were aware of any established procedures or reporting channels in the event of a data breach. Nevertheless, three participants expressed concern over potential unauthorized access to patient data, particularly if transmitted via messaging apps or stored in unencrypted cloud platforms. These findings indicate that healthcare workers' awareness remains confined to ethical boundaries, lacking legal and technical responsibility. The absence of internal training, weak access policies, and non-existent incident reporting mechanisms demonstrate that patient data protection has not yet become an integral part of the institutional culture in healthcare services.

b. Interview Findings from Policy Makers

Four policy makers were interviewed, consisting of two officials from local health departments and two legal staff from hospitals—one from a public institution and the other from a private facility. The interview questions focused on regulatory implementation, monitoring mechanisms, and internal policies related to patient data protection. All four acknowledged awareness of the enactment of Law No. 27 of 2022 on Personal Data Protection; however, none could specify any derivative documents, technical guidelines, or monitoring systems currently in place. One local health department officer stated, “We’re still waiting for official technical guidelines from the Ministry. For now, each hospital is doing things their own way.”

None of the respondents could present any internal audit systems related to patient data governance. In two of the institutions, current SOPs still refer to outdated regulations predating the PDP Law and have not been revised to include definitions of personal data, access control, or the designation of data protection responsibilities. One hospital legal officer admitted that the confidentiality clauses in employment contracts had not been updated since 2017 and made no reference to “personal data.” When asked about the existence of incident reporting procedures or mitigation plans in case of a breach, all informants stated that such documents or protocols did not yet exist. This suggests that the implementation of the PDP Law remains at the conceptual level, lacking structured enforcement and supervision mechanisms.

Nonetheless, the informants recognized the urgency of the issue and emphasized the need for technical training and inter-agency coordination to strengthen institutional capacity. Two of the four informants proposed that personal data protection be included as an indicator in hospital accreditation systems or reinforced through oversight by the Ministry of Health. Overall, these interviews reveal that

while policy makers understand the importance of data protection, the absence of legal and operational instruments remains a major barrier to real-world implementation.

c. Interview Findings from Information Technology Experts

Three IT experts were interviewed, including division heads and staff from two hospitals and one private clinic. The interview instrument focused on the state of information systems in use, the security features implemented, and challenges in managing patient digital data. All three experts stated that their institutions used locally customized SIMRS (Hospital Information Systems) provided by vendors, but lacked advanced security features such as data encryption, two-factor authentication, or audit trail management. When asked whether stored patient data received layered protection, all respondents answered no. One IT manager explained, "We do regular backups, but they're only saved to external hard drives and Google Drive—without additional passwords or encryption."

All participants confirmed that their login systems relied on standard username-password authentication without differentiated access levels among doctors, nurses, or administrative staff. None of the institutions had conducted any penetration testing or security audits within the past two years. When asked if there was a dedicated team or procedure to handle data breaches, they responded that any system disruption or access issue was addressed informally without official documentation. One staff member shared, "We've never had a major breach, but if anything happens, we just report it to the department head—there's no SOP."

All three experts highlighted that limited budgets, low digital literacy among users (doctors and nurses), and reliance on third-party vendors were the main obstacles to improving data security standards. They suggested that professional associations or authoritative bodies should assist institutions in designing information systems that are not only functional but also aligned with legal principles outlined in the PDP Law. These findings affirm that current digital health systems are not designed with security as a primary requirement.

d. Field Observation Findings

Field observations were conducted at four healthcare facilities—two regional hospitals and two private clinics in East Jakarta and Bekasi. The observations focused on both technical and non-technical aspects of patient data protection, including system access management, physical storage of medical records, and the presence of visual elements such as SOPs or confidentiality reminders. At one hospital, observers noted that a nurse station computer remained active and unattended for over 45 minutes, with no auto-logout system in place. Of the four institutions observed, only one used individual logins for medical personnel, while the remaining three relied on shared accounts within each unit. This practice compromises accountability and facilitates unauthorized access.

Physically, manual data entry was still observed at all facilities, especially in outpatient and follow-up services. Medical records were stored on open shelves without locks. At one clinic, documents related to HIV patients were kept in unlabelled folders in an unlocked staff desk drawer. None of the facilities had CCTV in medical record storage areas or administrative workspaces. No physical access logs or entry tracking documents were found for paper records. Only one hospital displayed a small poster regarding patient confidentiality at the registration desk; the others had no visual instructions or procedural reminders related to data security.

No SOPs were visibly posted in staff or administrative workspaces to explain data protection procedures explicitly. Incident reporting forms or information security violation forms were also unavailable. Suggestion boxes in patient waiting areas only contained feedback forms related to general service quality, with no option to report privacy concerns. Overall, these findings suggest that although digital systems are in use, there is no assurance that data protection principles are embedded in daily work behaviors or organizational culture at the facility level.

e. Document Analysis Findings

Twelve documents from the four institutions were reviewed, including internal policies, medical record SOPs, organizational structures, job descriptions, and patient registration forms. The aim was to assess the extent to which patient data protection had been integrated into official institutional documents. Of all documents analyzed, only one SOP from Hospital X explicitly mentioned "restricted access for authorized personnel to patient medical records," without technical details on who qualifies as authorized personnel, how access is granted or revoked, or who is responsible for overseeing the system. No documents mentioned the designation of roles such as Data Protection Officer (DPO) or data security management units within the institutional hierarchy.

Most SOPs focused on medical and administrative procedures—such as patient admission, medication distribution, and discharge protocols—without referencing data protection, breach reporting, or information leakage risk management. Available job descriptions only outlined general duties, with no mention of handling sensitive data or ensuring patient confidentiality. Even in "Employee Codes of Ethics" found in two hospitals, terms such as "personal data" or "electronic information protection" were entirely absent.

Patient registration forms in all facilities requested full identification data including NIK (citizen ID number), address, and health history, but none included written consent statements regarding data use or processing. Nor did they inform patients about their rights over personal data. No clauses mentioned data retention, third-party access, or the right to withdraw consent. These findings confirm that personal data protection regulations have not yet been substantively internalized within institutional documentation—legally, technically, or operationally.

Discussion

The finding that most healthcare professionals do not understand the core principles of the Personal Data Protection Law (UU PDP) illustrates a significant disconnect between regulatory developments and professional preparedness in the healthcare sector. A lack of legal literacy regarding data protection may impede the implementation of comprehensive information security standards. This aligns with the findings of Albrecht *et al*., who emphasized that legal understanding significantly influences privacy compliance among healthcare workers [16, 17]. When health professionals rely solely on ethical norms

without supporting legal awareness, the risk of data breaches increases due to the absence of accountability or recognition of formal obligations.

The limited availability of formal training further confirms that data protection has yet to be institutionalized within staff capacity-building programs. Legal awareness and technical competence are both critical foundations for developing an organizational culture of information security in hospitals [16]. Case-based training models that link privacy violations to real legal consequences have proven effective in enhancing staff compliance with patient data protection policies [17]. Without this type of approach, healthcare workers may continue to treat privacy as a secondary concern amidst daily clinical pressures.

This condition should serve as a call to action for healthcare facility managers to review and strengthen staff orientation and continuing education. Integrating data protection principles into both medical and administrative training can help bridge the gap between professional and legal responsibilities. This is not only essential for safeguarding patient rights, but also for reducing institutional legal risks in the event of data breaches [18, 19, 20].

Interviews with policymakers revealed that the absence of technical guidelines and weak internal audits have created a vacuum in the operationalization of patient data protection laws. This condition reflects what Greenhalgh *et al*. referred to as the "policy-practice gap" in digital healthcare, where regulations exist but fail to materialize due to weak institutional controls and a lack of operational instruments [21]. In the absence of clear standards, interpretation of the PDP Law becomes subjective and inconsistent across hospitals.

The unpreparedness of institutions to conduct data audits or revise legal documents indicates that data protection has not yet been embedded in institutional quality governance systems. In healthcare, information system audits and regulatory compliance assessments should be part of hospital risk management and accreditation procedures [22]. The World Health Organization (WHO) also emphasizes the need for cross-sectoral collaboration between legal, health, and IT actors to build safe digital health systems [23, 24]. Without such mechanisms, healthcare institutions remain vulnerable to legal non-compliance and security threats.

To bridge this gap, collaboration is needed between the government, professional associations, and institutional administrators to develop practical, operational guidelines. National regulations must be translated into internal documents such as SOPs, director decrees, and technical accreditation standards that can be implemented at the facility level [25]. This way, data protection becomes not only a personal obligation but also a structured component of institutional systems.

Findings from IT experts suggest that the Hospital Information Systems (SIMRS) currently used lack basic security features such as encryption, multi-factor authentication, and role-based access control. This indicates a dominance of functionality-oriented design over protective design in the development of healthcare information systems. Sharma *et al*. reported that systems not built upon "privacy by design" principles tend to fail in delivering real patient data protection [26]. Without security embedded from the outset, systemic vulnerabilities are unavoidable.

Institutional dependence on external vendors, without the capacity to conduct technical evaluations or internal audits, underscores a weakness in self-regulation of digital systems. Bărcanescu found that low IT literacy among hospital management is a major barrier to the secure and efficient adoption of healthcare technologies [27]. In Indonesia—where capacity disparities between facilities are significant—government support in the form of national standards or certification incentives is urgently needed.

One approach is to introduce mandatory certification for hospital software and provide regular technical training for internal IT teams. Strengthening in-house technical capabilities is key to transforming hospitals into institutions that are not only digitally operational but also legally and technologically secure [28]. Thus, information systems should serve as legal and ethical safeguards, not just data management tools. Observational data show that patient data protection has not yet been integrated into daily work routines in most health facilities. Shared accounts, inactive auto-logout settings, and unsecured medical record storage demonstrate a lack of awareness and technical discipline in managing sensitive information. Cruz *et al*. similarly concluded that successful data protection implementation depends more on cultural transformation than on technology availability [29]. If data privacy is not practiced, even well-equipped digital systems will fail to prevent violations.

The absence of visual aids such as reminder posters, displayed SOPs, or incident report forms further indicates that data protection is not yet internalized as an institutional value. Visual indicators in workspaces have been shown to increase staff awareness and compliance with privacy policies [30]. The lack of a manual or digital incident reporting system also means institutions cannot detect, document, or mitigate data breaches effectively. Without such documentation, systemic improvements remain unsupported by evidence. A shift in work culture toward data protection requires strong managerial support, continuous supervision, and positive reinforcement for staff compliance. It is also important to build internal monitoring systems that assess not only technical aspects but also behavioral patterns and workplace practices that pose security risks. This approach has been adopted successfully in European hospitals through "privacy governance frameworks" that assign collective responsibility for data protection to all operational units [31].

Document analysis confirms that most healthcare institutions have not embedded data protection principles into their policy structures or operational documentation. The absence of designated roles such as Data Protection Officers (DPOs), the lack of SOP clauses addressing breach management, and vague job descriptions point to the institutional neglect of this legal responsibility. Ahmed and Noor argue that formal documents explicitly addressing privacy are foundational to accountable data governance [32]. None of the documents reviewed mentioned patients' rights over their data—such as the right to know, access, correct, or withdraw consent for data usage. In international best practices, patient registration forms typically include consent declarations and information on data retention, access by third parties, and legal rights [33]. The absence of such clauses implies that institutions have not yet adopted the principles of "transparency and accountability" as recommended by both the GDPR and the Indonesian PDP Law. A comprehensive adjustment of institutional documentation is needed to comply with national law. This process must involve revising SOPs and forms, adapting

organizational structures, training staff to understand the updated materials, and integrating policies into audit and accreditation systems. As El Emam *et al*. emphasized, privacy policies must not remain as written documents—they must be lived and practiced throughout the institution [34, 35].

Conclusion

This study reveals that patient data protection mechanisms across healthcare facilities in Indonesia remain underdeveloped and inconsistently applied. Healthcare professionals demonstrate limited awareness of personal data protection principles, particularly those enshrined in Law No. 27 of 2022 on Personal Data Protection. In clinical practice, data security principles are not systematically integrated—either through institutional policies or formal training programs. The absence of incident reporting protocols, reliance on shared user accounts, and lack of digital literacy training underscore the broader absence of a data protection culture within health institutions. At the organizational level, institutions show limited capacity to translate regulatory mandates into actionable policies. No evidence of internal audits, standard technical guidelines, or formal assignment of data protection responsibilities was found. Key institutional documents such as standard operating procedures (SOPs), organizational charts, and patient service forms fail to incorporate core principles of transparency, accountability, and patient rights. To address these gaps, the study recommends a multi-pronged strategy. First, continuous education and awareness programs on data protection laws and ethical responsibilities should be institutionalized for healthcare personnel. Second, regulatory authorities must urgently develop and disseminate sector-specific technical guidelines to operationalize the PDP Law. Third, healthcare institutions should revise internal governance structures and SOPs to reflect data protection principles, including the designation of data protection officers and the establishment of incident response protocols. Fourth, investments should be directed toward enhancing hospital information systems with essential safeguards such as encryption, multi-factor authentication, and role-based access controls. Finally, regular audits and alignment with international data protection standards are essential to ensure not only legal compliance but also public trust in the secure handling of patient data.

References

1. Ienca M, Vayena E. On the responsible use of digital data to tackle the COVID-19 pandemic. Nat Med,2020:26(4):463–464.
2. Sweeney L. Only you, your doctor, and many others may know. Technol Sci, 2015, 2015092903.
3. Greenhalgh T, Wherton J, Papoutsi C. Beyond adoption: A new framework for theorizing and evaluating nonadoption, abandonment, and challenges to the scale-up of health and care technologies. J Med Internet Res,2017:19(11):e367.
4. Albrecht J, Kim D, Murdoch J. Understanding health data privacy laws: Legal knowledge and compliance in clinical settings. Health Policy,2020:124(4):501–509.
5. Zhang T, Yeoh E, Chiu M. Legal preparedness and workforce training for digital health privacy. BMC Health Serv Res,2020:20(1):881.
6. Samuel G, Lucassen A. Practical ethics training to improve staff response to data protection. J Med Ethics Educ,2021:17(1):22–30.
7. Rodrigues JJPC, de la Torre I, Fernández G, López-Coronado M. Analysis of the security and privacy requirements of cloud-based electronic health records systems. J Med Syst,2018:42(8):146.
8. Bărcanescu EM. The impact of IT literacy among healthcare administrators on data security implementation. Comput Hum Behav Rep,2021:4:100123.
9. Sharma R, Ramamurthy V. Design flaws in electronic medical record systems: A privacy-by-design perspective. Health Inf Sci Syst,2019:7(1):12.
10. World Health Organization. Digital health and privacy governance in low-resource settings: A guidance document. Geneva: WHO, 2021.
11. Jang H, Lee H. Operationalizing privacy laws in hospital SOPs: Lessons from comparative legal review. Health Policy Technol,2021:10(4):100559.
12. Cruz MJ, Silva A, Dias M. Embedding privacy in hospital operations: The behavioral dimension. Health Syst Policy Res,2020:7(1):54–60.
13. Landry MD, Raman SR. Using signage and visual management to improve data confidentiality compliance. J Healthc Qual,2020:42(2):75–83.
14. Christensen T, Lægreid P. Privacy governance frameworks in hospital management: Nordic case studies. Public Adm Rev,2021:81(4):632–643.
15. Ahmed R, Noor NM. Institutional documentation of data privacy: A Southeast Asian perspective. Asian Bioeth Rev,2020:12(3):275–289.
16. Langarizadeh M, Tabatabaei MS, Tavakol K. Consent forms in healthcare: Evaluating transparency and adequacy. Int J Health Plann Manage,2020:35(3):646–654.
17. Siregar RA. Hukum Kesehatan. Sinar Grafika, 2023.
18. El Emam K, Jonker E, Arbuckle L, Malin B. A systematic review of re-identification attacks on health data. PLoS One,2019:14(3):e0211993.
19. Metomic. A comprehensive guide to healthcare data security, 2023. Available from: https://www.metomic.io/resource-centre/a-comprehensive-guide-to-healthcare-data-securityMetomic
20. Siregar RA, Pandiangan HJ. Health Law Implementation Realizes Gender Equality and Women's Empowerment. Sociae Polites: Majalah Ilmu Sosial Politik,2023:24(2):88–95.
21. Siregar RA. A Legal Perspective on The Transformation of Health Services with Artificial Intelligence. Soepra Jurnal Hukum Kesehatan,2023:9(2):306–14.
22. National Committee on Vital and Health Statistics. Health information privacy beyond HIPAA: A framework for use and protection of health data, 2019. Available from: https://ncvhs.hhs.gov/wp-content/uploads/2019/07/Report-Framework-for-Health-Information-Privacy.pdfNCHS
23. Office of the Australian Information Commissioner. Guide to health privacy, 2018. Available from: https://www.oaic.gov.au/__data/assets/pdf_file/0011/2090/guide-to-health-privacy.pdfOAIC

24. U.S. Department of Health and Human Services. Informed consent FAQs, 2021. Available from: https://www.hhs.gov/ohrp/regulations-and-policy/guidance/faq/informed-consent/index.htmlHHS.gov
25. Siregar RA. Telemedicine Services of the Individual Health Rights in New Normal Era. Jurnal Hukum dan Peradilan,2021:10(2):300–14.
26. American Medical Association. Informed consent: Code of Medical Ethics Opinion 2.1.1, 2020. Available from: https://code-medical-ethics.ama-assn.org/ethics-opinions/informed-consentAMA Code of Medical Ethics
27. Choudhury O, Gkoulalas-Divanis A, Salonidis T, Sylla I, Park Y, Hsu G, *et al*. Differential privacy-enabled federated learning for sensitive health data. arXiv preprint, 2019. Available from: https://arxiv.org/abs/1910.02578arXiv
28. Ali M, Naeem F, Tariq M, Kaddoum G. Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. arXiv preprint, 2022. Available from: https://arxiv.org/abs/2203.09702arXiv
29. Asghar MR, Lee T, Baig MM, Ullah E, Russello G, Dobbie G. A review of privacy and consent management in healthcare: A focus on emerging data sources. arXiv preprint, 2017. Available from: https://arxiv.org/abs/1711.00546arXiv
30. Schulz A, Bohnet-Joschko S. Enhancing patient informed consent in elective skin cancer surgeries: A comparative study of traditional and digital approaches in a German public hospital. BMC Health Serv Res,2024:24(1):102.
31. Teare HJA, Morrison M, Whitley EA, Kaye J. Towards 'Engagement 2.0': Insights from a study of dynamic consent with biobank participants. Digital Health,2015:1:2055207615605644.
32. Mascalzoni D, Hicks A, Pramstaller P, Wjst M. Informed consent in the genomics era. PLoS Med,2010:7(7):e1000279.
33. Kaye J, Whitley EA, Lund D, Morrison M, Teare HJA. Dynamic consent: A patient interface for twenty-first century research networks. Eur J Hum Genet,2015:23(2):141–146.
34. Siregar RA. Telemedicine Services of the Individual Health Rights in New Normal Era. Jurnal Hukum dan Peradilan,2021:10(2):300–14.
35. Madathil KC, Koikkara R, Gramopadhye AK, Greenstein JS. An empirical study of the usability of consenting systems: iPad, touchscreen and paper-based systems. Proc Hum Factors Ergon Soc Annu Meet,2013:57(1):591–595.