Varians Jurnal Kesehatan Masyarakat

Volume 4 Issue 1, 2026
DOI: https://doi.org/10.63953/vjkm.v4i1.58
Website: https://jurnalvarians.com/index.php/vjkm

Tanggung Jawab Hukum dan Etika Atas Penyalahgunaan Data Pasien dalam Aplikasi Kesehatan: Sebuah Studi Literatur

Legal and Ethical Responsibilities for Patient Data Misuse in Healthcare Applications: A Literature Review

Nayla Inez Rachmawati[1*], Delima Oktafiya[2], Fabian Wahyu Aji[3], Een Kurnaesih[4]
[1,2,3,4] Kesehatan Masyarakat Program Sarjana, Fakultas Ilmu Kesehatan, UPN "Veteran" Jakarta
[*]Email Korespondensi: 2410713005@mahasiswa.upnvj.ac.id

INFO ARTIKEL

Article History
Received : 3 Desember 2025
Revised: 4 April 2026
Accepted : 2 Mei 2026

Kata Kunci:
Data pasien; Etika profesi medis; Kesehatan digital; Keamanan siber; Perlindungan data; UU PDP 2022.

Keywords:
Cybersecurity; Data protection; Digital health; Medical ethics; Patient data; Personal Data Protection Law (UU PDP 2022).

ABSTRAK

Penyalahgunaan data pasien dalam sistem kesehatan digital menimbulkan dampak serius terhadap privasi, kepercayaan publik, dan keberhasilan transformasi layanan kesehatan. Penelitian ini bertujuan untuk menganalisis integrasi aspek hukum, kesiapan teknologi, dan kepatuhan etika dalam tata kelola data pasien di Indonesia pasca-pemberlakuan UU PDP 2022, serta merumuskan strategi penguatan budaya keamanan data untuk meminimalisir risiko kebocoran informasi medis. Metode penelitian menggunakan studi literatur terhadap regulasi nasional, standar internasional, dan hasil penelitian akademik terkait perlindungan data kesehatan. Penelusuran artikel dilakukan melalui database PubMed, Scopus, Google Scholar, serta dokumen resmi dari Kementerian Kesehatan Republik Indonesia, Kominfo RI, WHO, dan ISO. Hasil kajian menunjukkan bahwa ancaman terhadap data pasien bersifat kompleks, meliputi risiko teknis seperti enkripsi lemah dan serangan malware, risiko privasi berupa penyalahgunaan data untuk tujuan komersial, risiko hukum terkait gap implementasi regulasi, serta risiko etika akibat lemahnya tata kelola lintas aktor. Pembahasan menegaskan bahwa teknologi memiliki peran ganda sebagai sumber risiko sekaligus solusi mitigasi, sementara regulasi hukum tidak akan efektif tanpa dukungan kapasitas teknis dan budaya keamanan siber tenaga medis. Kesimpulan penelitian ini menegaskan perlunya integrasi hukum, teknologi, dan etika yang konsisten, disertai strategi peningkatan literasi digital dan tata kelola etis untuk memperkuat kepercayaan masyarakat terhadap layanan kesehatan digital.

ABSTRACT

The misuse of patient data in digital health systems poses serious impacts on privacy, public trust, and the success of healthcare transformation. This study aims to analyze the integration of legal aspects, technological readiness, and ethical compliance in patient data governance in Indonesia after the enactment of the Personal Data Protection Law (UU PDP 2022), as well as to formulate strategies for strengthening data security culture to minimize the risk of medical information leakage. The research method employed a literature review of national regulations, international standards, and academic studies related to health data protection. Article searches were conducted through PubMed, Scopus, Google Scholar, and official documents from the Indonesian Ministry of Health, Ministry of Communication and Informatics, WHO, and ISO. The findings reveal that patient data threats are complex, including technical risks such as weak encryption and malware attacks, privacy risks involving data misuse for

e-ISSN 3048-0108

commercial purposes, legal risks due to regulatory implementation gaps, and ethical risks arising from weak governance across multiple actors. The discussion emphasizes that technology plays a dual role as both a source of risk and a mitigation solution, while legal regulations will not be effective without technical capacity and cybersecurity culture among medical staff. This study concludes that consistent integration of law, technology, and ethics, accompanied by strategies to improve digital literacy and ethical governance, is essential to strengthen public trust in digital health services.

PENDAHULUAN

Penyalahgunaan data pasien dalam aplikasi kesehatan digital menimbulkan dampak serius terhadap privasi, kepercayaan publik, dan martabat manusia. Kasus kebocoran data medis yang terjadi di berbagai negara menunjukkan bahwa informasi sensitif seperti identitas, riwayat penyakit, hingga data genetika dapat dimanfaatkan untuk tujuan komersial maupun diskriminatif.[11,23] Dampak yang muncul tidak hanya berupa kerugian hukum dan sosial, tetapi juga trauma psikologis bagi pasien yang merasa hak privasinya dilanggar.[11] Oleh karena itu, isu ini menjadi sangat mendesak untuk dikaji secara mendalam agar perlindungan data pasien dapat terjamin di tengah pesatnya transformasi layanan kesehatan berbasis teknologi.

Fenomena penyalahgunaan data pasien dalam aplikasi kesehatan tidak hanya terjadi di Indonesia, tetapi juga menjadi perhatian global. Laporan internasional menunjukkan bahwa sektor kesehatan merupakan salah satu target utama serangan siber karena protokol keamanannya relatif lemah dibandingkan sektor lain seperti perbankan.[12,24] Di Amerika Serikat, misalnya, pelanggaran terhadap regulasi HIPAA sering kali melibatkan kebocoran data medis yang berdampak pada jutaan pasien.[11] Sementara itu, di Uni Eropa, penerapan General Data Protection Regulation (GDPR) menegaskan pentingnya hak akses dan kendali pasien atas data medis mereka.[15] Di Indonesia sendiri, kasus kebocoran data pasien masih sering terjadi akibat lemahnya infrastruktur digital dan rendahnya budaya keamanan siber di kalangan tenaga kesehatan.[7,13] Fakta ini menunjukkan bahwa penyalahgunaan data pasien merupakan masalah lintas negara yang layak dikaji secara mendalam.

Dalam konteks regulasi, Indonesia telah memperkuat perlindungan data melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) serta Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 mengenai rekam medis elektronik.[16,18] Kerangka hukum ini memberikan dasar yang lebih komprehensif dibandingkan aturan sektoral sebelumnya. Namun, jika dibandingkan dengan standar internasional, Indonesia masih tertinggal. Uni Eropa telah menerapkan General Data Protection Regulation (GDPR) yang memberikan hak akses dan kendali penuh kepada pasien atas data medis mereka,[15] sementara Amerika Serikat memiliki Health Insurance Portability and Accountability Act (HIPAA) yang secara ketat mengatur kerahasiaan dan keamanan data kesehatan.[11] Perbedaan standar ini menunjukkan perlunya pembaruan tata kelola di Indonesia agar setara dengan praktik terbaik internasional.

Literatur sebelumnya banyak membahas digitalisasi kesehatan dari sisi regulasi normatif maupun hambatan teknis infrastruktur.[24] Namun, kajian yang secara khusus menyoroti keterkaitan antara kepatuhan hukum terhadap UU PDP 2022 dengan kesiapan budaya keamanan siber tenaga medis dalam ekosistem telemedicine masih sangat terbatas. Beberapa penelitian menekankan lemahnya budaya keamanan siber di kalangan tenaga kesehatan,[7] sementara studi lain menyoroti gap implementasi regulasi perlindungan data di fasilitas kesehatan.[13,20] Kekosongan kajian yang menghubungkan aspek hukum dan perilaku manusia inilah yang menjadi kebaruan penelitian ini. Oleh karena itu, tujuan artikel ini adalah menganalisis integrasi aspek hukum, kesiapan teknologi, dan kepatuhan etika dalam tata kelola data pasien di Indonesia pasca-pemberlakuan UU PDP, serta merumuskan strategi penguatan budaya keamanan data untuk meminimalisir risiko kebocoran informasi medis. Padahal, analisis irisan antara hukum dan perilaku manusia ini sangat penting karena regulasi yang ketat tidak akan berjalan efektif tanpa didukung oleh kesiapan etis dan perilaku aman dari para operator sistem kesehatan itu sendiri.[7]

Berdasarkan urgensi tersebut, penelitian ini bertujuan untuk menganalisis integrasi aspek hukum, kesiapan teknologi, dan kepatuhan etika dalam tata kelola data pasien di Indonesia pasca-pemberlakuan UU PDP, serta merumuskan strategi penguatan budaya keamanan data untuk meminimalisir risiko kebocoran informasi medis.

METODE

Penelitian ini menggunakan desain literature review yang bertujuan mengidentifikasi, menganalisis, dan mensintesiskan regulasi hukum, prinsip etika, serta temuan ilmiah terkait perlindungan data pasien dalam layanan kesehatan digital.[1,4] Pendekatan ini dipilih untuk memperoleh pemahaman komprehensif mengenai tantangan dan implikasi perlindungan informasi medis di era digital.[5,6]

Penelusuran literatur dilakukan melalui beberapa basis data utama, yaitu Google Scholar, PubMed, dan Scopus. Pencarian mencakup dua jenis sumber, yaitu regulasi dan pedoman resmi (UU PDP, Permenkes, WHO, ISO, GDPR, HIPAA) serta artikel penelitian akademik yang relevan. Proses pencarian menggunakan kombinasi kata kunci seperti digital health ethics, health data protection, medical data privacy regulation, HIPAA compliance, dan GDPR health data untuk memastikan cakupan publikasi yang komprehensif dan terkini.

Kriteria inklusi meliputi artikel akademik berbahasa Indonesia atau Inggris yang diterbitkan dalam 10 tahun terakhir dan membahas keamanan data, privasi medis, etika digital, rekam medis elektronik, atau regulasi perlindungan data kesehatan.[10,15]

Kriteria eksklusi terdiri dari artikel yang tidak relevan dengan isu perlindungan data kesehatan, publikasi yang tidak tersedia secara lengkap, serta artikel opini, berita, atau sumber non-ilmiah lainnya.[16]

Proses seleksi literatur dilakukan melalui tiga tahap, yaitu identifikasi artikel hasil pencarian awal, penyaringan judul dan abstrak berdasarkan relevansi topik, serta penilaian kelayakan artikel untuk dibaca secara penuh guna memastikan kesesuaian isi. Literatur yang memenuhi kriteria kemudian dianalisis lebih lanjut, mencakup regulasi dan pedoman resmi (UU PDP, Permenkes, WHO, ISO, GDPR, HIPAA) serta artikel hasil penelitian akademik dari database seperti PubMed, Scopus, dan Google Scholar.

Jenis literatur yang dianalisis mencakup regulasi formal di Indonesia seperti Undang-Undang Perlindungan Data Pribadi Tahun 2022[20], Permenkes terkait rekam medis elektronik[21], dan kebijakan transformasi digital kesehatan[22]; artikel hasil riset nasional dan internasional yang membahas keamanan data, risiko kebocoran, etika digital, dan kerangka hukum perlindungan data;[23,24] serta sumber pendukung seperti standar internasional keamanan informasi.[25]

Analisis data dilakukan dengan pendekatan naratif tematik melalui tahapan mengidentifikasi tema utama dari setiap literatur, membandingkan regulasi Indonesia dengan standar internasional seperti GDPR dan HIPAA,[7,9] serta menelaah prinsip etika kesehatan yang terkait dengan pengelolaan informasi medis.[23,24] Pendekatan ini memungkinkan peneliti memperoleh gambaran menyeluruh mengenai interaksi antara teknologi, regulasi, dan etika dalam menjaga keamanan informasi pasien.

HASIL

Berdasarkan proses pencarian literatur melalui Google Scholar, PubMed, dan Scopus dengan kata kunci yang telah ditetapkan, diperoleh sejumlah artikel yang memenuhi kriteria inklusi, yaitu membahas keamanan data, privasi medis, etika digital, rekam medis elektronik, serta regulasi perlindungan data kesehatan. Setelah melalui tahap penyaringan judul, abstrak, dan pembacaan penuh, artikel yang relevan dianalisis secara tematik. Hasil analisis menunjukkan adanya lima kelompok risiko utama yang konsisten muncul dalam berbagai sumber, yaitu risiko teknis, risiko privasi, risiko kebocoran data, risiko penyalahgunaan data, dan risiko tata kelola.

Hasil penelusuran literatur menunjukkan bahwa perlindungan data pasien dalam pelayanan kesehatan digital dipengaruhi oleh berbagai faktor yang saling berkaitan. Risiko muncul bukan hanya dari aspek teknologi, tetapi juga dari prosedur operasional, kompetensi sumber daya manusia, serta kebijakan internal lembaga kesehatan. Secara menyeluruh, terdapat lima kelompok risiko utama yang paling sering ditemukan, yaitu risiko teknis, risiko privasi, risiko kebocoran data, risiko penyalahgunaan data, dan risiko tata

kelola.[6,12,13,24] Rangkuman kategori risiko tersebut ditampilkan pada Tabel 1.

Berdasarkan temuan lebih rinci, setiap kategori risiko memiliki bentuk risiko spesifik yang dapat menimbulkan implikasi berbeda terhadap perlindungan data[12,13,24]. Ringkasan jenis risiko, bentuk risiko, dan dampaknya digambarkan pada Tabel 2.

Tabel 1. Kategori Risiko dalam Perlindungan Data Pasien di Sistem Kesehatan Digital

Kategori Risiko	Deskripsi Singkat
Risiko Teknis	Risiko yang timbul akibat kelemahan sistem, bug, kesalahan konfigurasi, atau serangan siber yang menargetkan infrastruktur digital kesehatan.[12,24]
Risiko Privasi	Risiko terkait pengelolaan data pribadi yang tidak sesuai prinsip minimisasi data, persetujuan, serta hak kontrol pasien[11,15,18]
Risiko Kebocoran Data	Risiko data pasien diakses, dipindahkan, atau disebarkan oleh pihak yang tidak berwenang.[6,13]
Risiko Penyalahgunaan Data	Potensi pemanfaatan data pasien untuk tujuan non-medis, seperti komersial, politis, atau diskriminatif.[1,13]
Risiko Tata Kelola	Risiko yang muncul akibat ketidaktepatan kebijakan, lemahnya SOP, kurangnya pelatihan, atau rendahnya pengawasan internal.[16,17,20]

Tabel 2. Bentuk Risiko dan Dampaknya terhadap Perlindungan Data Pasien

Jenis Risiko	Bentuk Risiko	Dampak terhadap Perlindungan Data
Risiko Teknis	Kerentanan aplikasi, server tidak terenkripsi, pembaruan sistem tidak rutin[12,24]	Meningkatkan peluang peretasan, hilangnya data, atau akses ilegal terhadap data pasien.
Risiko Privasi	Pengumpulan data berlebihan, akses internal yang tidak dibatasi[11,15,18]	Mengurangi kendali pasien terhadap data pribadi dan berpotensi melanggar kerahasiaan medis
Risiko Kebocoran Data	Insiden phishing, ransomware, paparan cloud, salah kirim berkas[6,13]	Data pasien dapat tersebar luas dan menimbulkan dampak sosial, psikologis, maupun hukum.
Risiko Penyalahgunaan Data	Penggunaan data untuk iklan, profiling, atau kepentingan lembaga[1,13]	Mengancam hak dan martabat pasien serta menurunkan kepercayaan publik terhadap sistem kesehatan digital.
Risiko Tata Kelola	SOP tidak lengkap, kurangnya audit, minim pelatihan tenaga kesehatan[16,17,20]	Implementasi perlindungan data menjadi tidak konsisten dan rawan pelanggaran.

Hasil yang ditampilkan dalam dua tabel tersebut menunjukkan bahwa risiko perlindungan data pasien tidak bersifat tunggal, melainkan saling bertaut dan saling memperkuat. Risiko teknis dan privasi tampak paling dominan dalam berbagai sumber literatur, terutama pada sistem yang telah mengimplementasikan pencatatan kesehatan elektronik dan integrasi data lintas layanan [12,24]. Selain itu, risiko tata kelola tampil sebagai

faktor pentingkegagalan perlindungan data pada tingkat institusi.[16,17,20]

Temuan pada Tabel 2 menunjukkan bahwa bentuk risiko yang bersumber dari kelemahan sistem, prosedur internal, maupun faktor manusia dapat meningkatkan peluang terjadinya insiden keamanan. Kelemahan teknis seperti kurangnya enkripsi dan pembaruan sistem yang tidak konsisten cenderung menjadi penyebab awal terjadinya pelanggaran data. Sementara itu, risiko privasi dan penyalahgunaan data terutama muncul ketika akses terhadap data pasien tidak diatur secara ketat dan transparan.[11,15,18]

Secara keseluruhan, hasil ini menggambarkan bahwa perlindungan data pasien dalam sistem kesehatan digital dipengaruhi oleh kombinasi aspek teknis, operasional, dan tata kelola. Keragaman risiko yang ditemukan menjadi dasar penting untuk melakukan analisis lebih lanjut pada bagian pembahasan terkait bagaimana strategi dan pendekatan dapat diperkuat untuk meningkatkan keamanan data pasien di era digital.[12,13,24]

Dengan demikian, hasil kajian literatur ini menegaskan bahwa risiko perlindungan data pasien tidak bersifat tunggal, melainkan saling berkaitan. Temuan ini sesuai dengan tema utama yang ditetapkan dalam metode penelitian, yaitu integrasi aspek hukum, etika, dan teknologi dalam perlindungan data pasien.

PEMBAHASAN

Pembahasan hasil penelitian menunjukkan bahwa ancaman terhadap data pasien dalam sistem kesehatan digital bersifat kompleks dan saling berkaitan. Pembahasan ini memperdalam hasil analisis literatur yang ditampilkan pada Tabel 1 dan Tabel 2, dengan menjelaskan implikasi dari setiap kategori risiko terhadap perlindungan data pasien.

Seperti ditunjukkan pada Tabel 1, kerentanan teknis seperti enkripsi yang tidak memadai, serangan malware, kurangnya pembaruan sistem, dan konfigurasi yang salah merupakan ancaman yang sering muncul. Hasil ini sejalan dengan temuan Elhoseny et al.[12] yang menyebutkan bahwa kelemahan teknis pada infrastruktur e-health termasuk server tidak terenkripsi dan pembaruan yang tidak konsisten menjadi penyebab utama insiden pelanggaran data. Selain itu, Vartiainen & Ewoh[24] juga menegaskan bahwa sektor kesehatan merupakan target serangan siber paling rentan karena kompleksitas ekosistem digitalnya.

Seperti ditunjukkan pada Tabel 2, risiko privasi dan penyalahgunaan data berdampak langsung pada kepercayaan publik dan kondisi psikologis pasien. Misalnya, penyalahgunaan data untuk tujuan komersial dapat memicu stigma, diskriminasi, dan berkurangnya rasa aman. Penelitian Balkin[11] menunjukkan bahwa data kesehatan memiliki karakteristik sensitif yang membuat penyalahgunaannya menimbulkan dampak psikologis yang lebih berat dibanding jenis data lainnya. Susilowati et al.[23] juga menemukan bahwa pelanggaran kerahasiaan medis secara langsung mengurangi kepercayaan publik terhadap fasilitas kesehatan.

Temuan pada Tabel 1 juga memperlihatkan bahwa risiko tata kelola muncul dari lemahnya SOP dan audit internal. Regulasi Indonesia sudah membentuk kerangka perlindungan data melalui UU PDP,[18] Permenkes 24/2022,[16] dan UU Kesehatan 2023. Namun, berbagai literatur menegaskan adanya gap implementasi. Hendra et al.[13] menyatakan bahwa banyak fasilitas kesehatan belum sepenuhnya menerapkan prinsip perlindungan data karena keterbatasan infrastruktur digital dan SOP yang belum memadai. Temuan penelitian ini juga sejalan dengan Lukitasari et al.[20] yang menyoroti bahwa tanggung jawab hukum rumah sakit terhadap penyalahgunaan data pasien masih lemah akibat rendahnya audit internal dan tidak adanya penegakan disiplin yang konsisten. Selain itu, Jannah et al.[15] membandingkan Indonesia dengan Uni Eropa dan menemukan bahwa standar perlindungan data Indonesia masih tertinggal dari GDPR, terutama terkait hak akses dan pengendalian pasien terhadap datanya.

Seperti ditunjukkan pada Tabel 1, risiko tata kelola juga terkait dengan aspek etika. Perlindungan data tidak bisa hanya mengandalkan tenaga medis. Ekosistem digital melibatkan pengembang aplikasi, penyedia cloud, analis data, dan vendor teknologi lainnya. WHO[21] menekankan bahwa semakin banyak aktor yang terlibat dalam rantai pengolahan data, semakin besar kebutuhan akan tata kelola etis yang mengatur transparansi, akuntabilitas, dan minimisasi risiko. Hal ini konsisten dengan Balkin[11] yang menegaskan bahwa penyedia

layanan digital harus diperlakukan sebagai information fiduciaries yang memiliki kewajiban moral dan hukum untuk menjaga data pasien secara ketat.

Seperti ditunjukkan pada Tabel 2, teknologi memiliki peran ganda: menjadi sumber risiko sekaligus solusi mitigasi. Kerentanan teknis dapat memicu kebocoran data, namun teknologi seperti enkripsi kuat, audit digital, anonimisasi, hingga blockchain dapat meningkatkan keamanan bila diterapkan dengan benar. ISO/IEC 27001:2022[14] merekomendasikan penguatan kontrol keamanan, termasuk manajemen risiko, kontrol akses, dan proteksi data lintas jaringan. Selain itu, WHO[21] merekomendasikan penerapan prinsip human oversight pada sistem kecerdasan buatan untuk mencegah penyalahgunaan data pasien di era digital yang semakin otomatis.

Temuan pada Tabel 1 juga menegaskan bahwa tantangan struktural seperti rendahnya literasi digital tenaga kesehatan, minimnya tenaga ahli keamanan siber, dan belum tersusunnya aturan turunan UU PDP 2022 semakin memperumit kondisi ini. Santhi[4] menekankan bahwa kesenjangan antara regulasi dan implementasi menjadi penyebab utama kebocoran data di fasilitas kesehatan Indonesia. Produk-produk layanan kesehatan digital yang menggunakan server luar negeri juga menimbulkan persoalan baru terkait kedaulatan data, sebagaimana dibahas oleh Küzeci[19] dalam konteks perlindungan data lintas negara.

Secara keseluruhan, pembahasan ini menunjukkan bahwa hasil kajian literatur tidak hanya bersifat deskriptif, tetapi juga menegaskan perlunya integrasi hukum, teknologi, dan etika agar perlindungan data pasien dapat berjalan efektif. Hal ini sekaligus memperkuat kebaruan penelitian, yaitu analisis irisan antara regulasi hukum dan perilaku manusia dalam ekosistem kesehatan digital.

KESIMPULAN DAN SARAN

Penelitian ini menyimpulkan bahwa perlindungan data pasien dalam layanan kesehatan digital merupakan isu multidimensi yang dipengaruhi oleh faktor teknis, kebijakan, tata kelola, serta prinsip etika profesi. Risiko kebocoran dan penyalahgunaan data tidak hanya bersumber dari kelemahan sistem informasi, tetapi juga dari minimnya pengawasan internal, rendahnya literasi privasi digital, dan ketidakkonsistenan implementasi regulasi. Temuan ini menegaskan bahwa regulasi hukum seperti UU PDP 2022 dan UU Kesehatan 2023 tidak akan berjalan efektif tanpa dukungan kesiapan teknologi dan budaya keamanan siber tenaga medis. Dengan demikian, tujuan penelitian untuk menganalisis integrasi aspek hukum, kesiapan teknologi, dan kepatuhan etika dalam tata kelola data pasien telah tercapai. Upaya perlindungan data ke depan membutuhkan komitmen etis yang konsisten, penguatan kapasitas tata kelola, serta strategi peningkatan literasi digital agar risiko kebocoran informasi medis dapat diminimalisir.

UCAPAN TERIMA KASIH

Penyusunan artikel ini dapat terlaksana berkat dukungan dari berbagai pihak yang telah berkontribusi dalam proses penelitian dan penulisan. Penulis mengucapkan terima kasih kepada institusi dan bagian terkait yang telah menyediakan dukungan akademik serta akses referensi yang dibutuhkan. Apresiasi juga disampaikan kepada pengajar mata kuliah Etika dan Hukum Kesehatan atas arahan dan pengetahuan yang diberikan selama perkuliahan, sehingga menjadi dasar penting dalam pengembangan kajian ini.

Penulis turut menghargai kerja sama seluruh anggota kelompok yang berperan dalam diskusi, pengumpulan literatur, dan penelaahan materi secara komprehensif. Selain itu, penghargaan diberikan kepada para profesional dan peneliti yang karyanya menjadi rujukan ilmiah dan turut memperkaya analisis dalam artikel ini. Tanpa kontribusi dan dukungan dari seluruh pihak tersebut, penyusunan penelitian ini tidak akan terselesaikan dengan baik.

DAFTAR PUSTAKA

1. Juwono V. Comparative review of personal data protection policy in Indonesia and the European Union General Data Protection Regulation. Publik (Jurnal Ilmu Administrasi). 2022 Dec 30.
2. Dewi TS, Silva AA. Hambatan implementasi rekam medis elektronik dari perspektif perekam medis dengan metode PIECES. J Manaj Inform Kesehat Indones. 2023 Oct 6;11(2).
3. Rama BG, et al. Protection of patient data confidentiality in telemedicine services in

Indonesia: A human rights perspective. Legal Brief. 2025 Jun 19;14(2):278–85.
4. Santhi NN. Patient data privacy challenges in electronic health systems: A juridical analysis of medical information protection in Indonesia. West Sci Law Hum Rights. 2025;3(1):1–8.
5. Bonsapia M. Aspek hukum telemedicine di Indonesia. The Juris. 2025 Jun 30;9(1):259–68.
6. Olofinbiyi SA. Cyber insecurity in the wake of COVID-19: a reappraisal of impacts and global experience within the context of routine activity theory. SciRise Jurid Sci. 2022 Mar 31;1(19):37–45.
7. Irwandy I, Ady Mangilep AU, Anggraeni R, Noor NB, Niartiningsih A, Latifah N, et al. Cybersecurity culture among healthcare workers in Indonesia: Knowledge gaps, demographic influences, and strategic policy solutions. Research Square [Preprint]. 2024 Dec 17. doi:10.21203/rs.3.rs-5421169/v1
8. Irwandy I, et al. Hospital size and cybersecurity practices: Evaluating nurses' awareness in Indonesia. J Public Health Pharm. 2025 Oct 2;5(3):616–26.
9. Dewayanti I, Suryono A. Tinjauan etika dan hukum praktik kedokteran melalui telemedicine pasca pandemi COVID-19. J Huk Pembang Ekon. 2023;11(1):27–40.
10. Arfah NA, Puspitosari H. Perlindungan hukum terhadap data pasien telemedicine dalam menerima pelayanan medis berbasis online. J Syntax Fusion. 2023;3:658–68.
11. Balkin JM. Information fiduciaries and the digital protection of health data. Yale Law J. 2020;129(6):1362–1405.
12. Elhoseny M, et al. Security and privacy issues in medical Internet of Things: Overview, countermeasures, challenges, and future directions. Sustainability. 2021;13(21):11645. doi:10.3390/su132111645
13. Hendra H, et al. E-health personal data protection in Indonesia. J Huk Kesehat Indones. 2022;1(2). doi:10.53337/jhki.v1i02.15
14. ISO/IEC. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO/IEC; 2022.
15. Jannah M, et al. Personal data protection in telemedicine: Comparison of Indonesian and European Union law. J Law Policy Transform. 2024;8(2). doi:10.37253/jlpt.v8i2.8827
16. Kementerian Kesehatan Republik Indonesia. Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. Jakarta: Kemenkes RI; 2022.
17. Kementerian Kesehatan Republik Indonesia. Strategi Transformasi Digital Kesehatan Nasional. Jakarta: Kemenkes RI; 2023.
18. Kementerian Komunikasi dan Informatika Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Jakarta: Kominfo RI; 2022.
19. Küzeci E. Personal data protection law. In: Introduction to Turkish Business Law. 2022:457–483.
20. Lukitasari DA, et al. Hospital legal responsibilities for misuse of patient personal data in electronic medical records. J Indones Law Policy Rev. 2023;5(1):60–74. doi:10.56371/jirpl.v5i1.164
21. World Health Organization. Ethics and governance of artificial intelligence for health: WHO guidance. Geneva: WHO; 2021.
22. Santhi NNP. Patient data privacy challenges in electronic health systems: A juridical analysis of medical information protection in Indonesia. West Sci Law Hum Rights. 2025;3(1):1–8.
23. Susilowati I, et al. Perlindungan hukum terhadap hak privasi dan data medis pasien di Rumah Sakit X Surabaya. J Wiyata. 2018;5.
24. Vartiainen P, Ewoh T. Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review. J Med Internet Res. 2024;26:e11179043.
25. Wahyuntara JK, et al. Pelindungan hak atas rahasia medis pasien dalam implementasi rekam medis elektronik (Studi pada RS Bhayangkara, Semarang). Soepra J Huk Kesehat. 2024;10(1):158–175.