

PERAN RUMAH SAKIT SEBAGAI PENGENDALI DATA DALAM MENJAMIN KEAMANAN DATA PRIBADI PASIEN PADA SISTEM KESEHATAN DIGITAL

Gunawan Widjaja

Senior Lecturer Faculty of Law Universitas 17 Agustus 1945 Jakarta
widjaja_gunawan@yahoo.com

Wagiman

Senior Lecturer Faculty of Law Universitas 17 Agustus 1945 Jakarta
wagimanmartedjo68@gmail.com

Dyah Ersita Yustanti

Senior Lecturer Faculty of Law Universitas 17 Agustus 1945 Jakarta
dyustanti@yahoo.com

Hotmaria Hertawaty Sijabat

Researcher, Faculty of Law Universitas 17 Agustus 1945 Jakarta
sijabathotmaria@gmail.com

Handojo Dhanudibroto

Doctoral Student, Faculty of Law Universitas 17 Agustus 1945 Jakarta
nonowango603@gmail.com

Abstract

Digital transformation in the health sector has brought various conveniences and efficiencies in patient data management, but it has also posed new challenges related to data security and privacy. Hospitals play an important role as data controllers responsible for ensuring that every process of collecting, storing, processing, and distributing patient data remains in accordance with the principles of security and confidentiality. This study aims to analyse the role of hospitals as data controllers in ensuring the protection of patient personal data in digital health systems, as well as to identify challenges and control strategies. The study was conducted through a literature review of various journals, regulations, and reliable documents, using a descriptive-qualitative approach. The results of the study indicate that data protection requires collaboration between the implementation of security technologies (encryption, two-factor authentication, audit trails), compliance with regulations, standardisation of operational procedures, and improvement of digital literacy among human resources. The main challenges include cyber threats, infrastructure and human resource limitations, and suboptimal data security culture. Systematic and continuous efforts in strengthening policies, education, and internal supervision are key to the success of hospitals as data controllers in the evolving era of digital health.

Keywords: Patient Data Security, Hospitals, Data Controllers, Digital Health Systems, Personal Data Protection

Abstrak

Transformasi digital pada sektor kesehatan telah menghadirkan berbagai kemudahan dan efisiensi dalam pengelolaan data pasien, namun juga menimbulkan tantangan baru terkait keamanan dan privasi data pribadi. Rumah sakit memegang peran penting sebagai pengendali data (*data controller*) yang bertanggung jawab dalam menjamin setiap proses pengumpulan, penyimpanan, pengolahan, serta distribusi data pasien tetap sesuai dengan prinsip keamanan dan kerahasiaan. Penelitian ini bertujuan untuk menganalisis peran rumah sakit sebagai pengendali data dalam menjamin perlindungan data pribadi pasien pada sistem kesehatan digital, serta mengidentifikasi tantangan dan strategi pengendaliannya. Kajian dilakukan melalui studi pustaka pada berbagai jurnal, regulasi, dan dokumen terpercaya, dengan pendekatan deskriptif-kualitatif. Hasil telaah menunjukkan bahwa perlindungan data membutuhkan kolaborasi antara penerapan teknologi keamanan (enkripsi, autentikasi ganda, audit trail), kepatuhan pada regulasi, standarisasi prosedur operasional, serta peningkatan literasi digital sumber daya manusia. Tantangan utama meliputi ancaman siber, keterbatasan infrastruktur dan SDM, serta budaya keamanan data yang belum optimal. Upaya sistematis dan berkelanjutan dalam penguatan kebijakan, edukasi, serta pengawasan internal menjadi kunci keberhasilan rumah sakit sebagai pengendali data di era kesehatan digital yang terus berkembang.

Kata Kunci: Keamanan Data Pasien, Rumah Sakit, Pengendali Data, Sistem Kesehatan Digital, Perlindungan Data Pribadi

Pendahuluan

Transformasi digital di bidang kesehatan telah menjadi pendorong utama dalam efisiensi dan peningkatan mutu layanan kesehatan di Indonesia. Penerapan sistem kesehatan digital, khususnya Rekam Medis Elektronik (RME), telah mengubah cara rumah sakit menyimpan, mengelola, dan membagikan data pasien. Inovasi ini tak hanya membawa manfaat, tetapi juga tantangan signifikan, terutama terkait dengan keamanan data pribadi pasien yang semakin menjadi isu krusial di era digital saat ini (Annan, 2024).

Kehadiran RME dan aplikasi kesehatan digital membuka peluang akses layanan yang lebih cepat, akurat, dan terintegrasi antar fasilitas kesehatan. Namun, dibalik kemudahan tersebut, muncul potensi risiko penyalahgunaan dan kebocoran data pribadi pasien. Masyarakat menjadi semakin khawatir atas privasi dan keamanan informasi medis mereka, mengingat seringnya terjadi insiden pencurian dan penyebaran data yang tidak bertanggung jawab (Rahma & Supriyadi, 2024).

Rumah sakit, sebagai lembaga layanan kesehatan, bertanggung jawab penuh atas perlindungan data pasien. Berperan sebagai pengendali data (*data controller*), rumah sakit tidak hanya wajib mematuhi regulasi, tetapi juga harus membangun sistem internal yang menjamin kerahasiaan, integritas, ketersediaan, serta keaslian data pasien (Rimbun et al., 2024). Regulasi terkait keamanan data di Indonesia semakin diperkuat dengan hadirnya Undang-Undang Perlindungan Data Pribadi (UU PDP) serta peraturan

Kementerian Kesehatan seperti Permenkes No. 24/2022. Regulasi ini mengamanatkan bahwa data pasien harus diperlakukan dengan standar keamanan tinggi, baik dari sisi teknis, prosedural, maupun sumber daya manusia yang mengelola data tersebut (*Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*, 2022, p. 24).

Berbagai permasalahan kerap ditemukan dalam implementasi keamanan data di rumah sakit, mulai dari akses tidak sah ke sistem RME, kelalaian petugas dalam menjaga kerahasiaan username dan password, hingga kurangnya SOP yang tegas mengenai distribusi dan penyimpanan data medis. Hal ini rentan membuka celah bagi pihak tak berwenang untuk memanfaatkan data pasien secara ilegal (Yuliana, 2021).

Aspek keamanan data tidak hanya mencakup kerahasiaan, melainkan pula integritas, autentikasi, ketersediaan, kontrol akses, hingga *non-repudiation* (nir-sangkal). Setiap aspek menuntut perhatian khusus dari rumah sakit agar mampu menghadirkan perlindungan data yang menyeluruh. Otentikasi ganda, enkripsi data, audit trail, dan pembatasan hak akses menjadi bagian kritis yang harus diterapkan (Pramukars, 2021). Tantangan yang dihadapi rumah sakit semakin kompleks dengan berkembangnya teknologi digital. Tidak hanya ancaman dari eksternal, namun juga dari internal seperti lemahnya budaya keamanan IT di lingkungan kerja, kurangnya edukasi bagi tenaga medis, serta keterbatasan sumber daya manusia yang kompeten dalam teknologi informasi (Dalimunthe, 2024).

Insiden-insiden kebocoran data di rumah sakit membuktikan pentingnya peran aktif rumah sakit dalam melakukan pengawasan serta pengendalian data secara berkala. Studi kasus di berbagai rumah sakit menunjukkan bahwa ketidakpatuhan prosedur, serta lemahnya pengelolaan akses dan password, menjadi penyebab utama rawannya kebocoran data pasien. Untuk mengatasi tantangan tersebut, dibutuhkan strategi keamanan berlapis, mulai dari penggunaan teknologi terkini hingga pembentukan SOP yang ketat (Putri, 2023). Selain itu, implementasi teknologi autentikasi seperti tanda tangan digital dan VPN untuk membatasi akses jaringan, menjadi solusi yang kini banyak diadopsi dalam menjaga keamanan data kesehatan. Kesadaran masyarakat akan hak perlindungan data pribadi juga berperan vital. Rumah sakit wajib melibatkan pasien dalam pengambilan keputusan terkait penggunaan dan pemanfaatan data mereka, serta memberikan edukasi mengenai resiko dan hak akses yang mereka miliki (Nurhayati, 2025).

Upaya perlindungan data juga harus dikombinasikan dengan audit dan evaluasi secara berkala terhadap sistem informasi yang digunakan. Audit ini penting untuk memetakan potensi risiko, serta untuk memastikan bahwa seluruh kebijakan dan sistem pengelolaan data berjalan sesuai dengan ketentuan regulasi yang berlaku.

Penelitian ini dilakukan untuk menganalisis lebih dalam peran rumah sakit sebagai pengendali data dalam menjamin keamanan data pribadi pasien di sistem kesehatan digital. Kajian pustaka menjadi metode yang dipilih guna mengumpulkan bukti dan praktik terbaik serta tantangan yang dihadapi oleh rumah sakit di Indonesia,

sekaligus memberikan rekomendasi konkret untuk perbaikan tata kelola data ke depan. Dengan penguatan peran rumah sakit sebagai pengendali data, diharapkan perlindungan dan keamanan data pribadi pasien semakin terjamin, sehingga dapat meningkatkan kepercayaan masyarakat terhadap layanan kesehatan digital dan mendukung transformasi digital sektor kesehatan secara berkelanjutan.

Metode Penelitian

Penelitian ini menggunakan metode kajian pustaka (*literature review*), yakni menelaah dan menganalisis secara sistematis berbagai sumber literatur yang relevan dengan peran rumah sakit sebagai pengendali data dalam menjamin keamanan data pribadi pasien pada sistem kesehatan digital (Eliyah & Aslan, 2025). Sumber data diperoleh dari jurnal ilmiah, regulasi pemerintah, buku, dan laporan kasus, yang dipilih berdasarkan kriteria relevansi dengan topik penelitian. Proses penelitian meliputi identifikasi topik, eksplorasi dan seleksi literatur, analisis kritis terhadap temuan utama, serta penyusunan sintesis naratif yang menggambarkan permasalahan, tantangan, dan praktik terbaik perlindungan data pasien di rumah sakit. Teknik pengumpulan data dilakukan melalui studi dokumentasi, sedangkan analisis data bersifat deskriptif-komparatif serta mengacu pada perkembangan regulasi dan hasil penelitian mutakhir di bidang keamanan data Kesehatan (Ferrari, 2020).

Hasil dan Pembahasan

Peran Rumah Sakit Sebagai Pengendali Data Dalam Menjamin Keamanan Data Pasien

Rumah sakit memegang peran sentral sebagai pengendali data dalam sistem kesehatan digital, terutama dalam melindungi keamanan dan privasi data pasien. Tugas ini bukan hanya aspek administratif, melainkan juga kewajiban hukum dan etika yang harus dilaksanakan secara konsisten di tengah pesatnya perkembangan teknologi Kesehatan (Wahyudin, 2025). Sebagai pengendali data, rumah sakit bertanggung jawab mengelola seluruh siklus data pasien, mulai dari pengumpulan, penyimpanan, penggunaan, hingga pemusnahan data. Setiap proses harus berjalan sesuai standar perlindungan data pribadi dan ketentuan perundangan—khususnya Undang-Undang Perlindungan Data Pribadi (UU PDP) serta regulasi sektoral seperti Permenkes No. 24/2022 tentang Rekam Medis Elektronik (Syarifuddin, 2024).

Kepatuhan terhadap aturan hukum sangat krusial. Rumah sakit wajib memastikan bahwa pemrosesan data pasien hanya dilakukan atas dasar persetujuan yang sah, transparansi informasi kepada pasien, serta akuntabilitas atas setiap aktivitas data yang terjadi di lingkungan rumah sakit (Lestari, 2020).

Data kesehatan yang ditangani rumah sakit bersifat sangat sensitif, meliputi data identitas diri, riwayat penyakit, hasil pemeriksaan, dan terapi medis. Kebocoran informasi ini dapat berdampak buruk tidak hanya pada kerahasiaan, tetapi juga pada keamanan dan reputasi pasien (Yusriadi, 2025). Oleh karena itu, hanya petugas yang

berwenang dan memiliki hak akses tertentu yang boleh mengakses data tersebut sesuai prinsip hak akses minimal. Keamanan data pasien harus diterapkan secara komprehensif, melalui kombinasi langkah teknis dan organisasional. Langkah teknis meliputi penggunaan sistem informasi terenkripsi, autentikasi ganda bagi pengguna sistem, audit akses berkala, serta backup data otomatis untuk menjaga ketersediaan dan integritas informasi.

Dari sisi organisasional, rumah sakit wajib menyusun dan menegakkan standar operasional prosedur (SOP) pengelolaan data. Pelatihan keamanan data secara rutin kepada seluruh staf rumah sakit, dari manajemen hingga tenaga kesehatan, menjadi bagian penting dalam membangun budaya perlindungan data yang kuat (Algifari, 2024).

Implementasi perlindungan data pasien di rumah sakit memerlukan sistem manajemen keamanan informasi yang terstandarisasi. Sertifikasi seperti ISO/IEC 27001 dapat menjadi acuan dalam membangun sistem tata kelola keamanan informasi yang profesional dan dapat diaudit secara periodik.

Infrastruktur teknologi rumah sakit juga harus menunjang keamanan data. Penggunaan server yang terenkripsi, firewall, sistem deteksi intrusi, serta pengelolaan jaringan internal yang baik, menjadi elemen vital untuk mengurangi kerentanan terhadap serangan siber atau akses ilegal oleh pihak yang tidak berwenang (Purnama, 2024).

Dasar hukum pengendalian data di rumah sakit menegaskan perlunya prinsip transparansi dan hak pasien. Pasien berhak mendapat kejelasan identitas, tujuan pengumpulan data, hingga akses terhadap data mereka sendiri. Setiap pelanggaran, baik oleh internal maupun eksternal rumah sakit, dapat dikenai sanksi administratif, pidana, atau gugatan perdata (Bonsapia & Jumiran, 2025). Salah satu tantangan besar adalah rendahnya literasi keamanan digital di kalangan tenaga kesehatan, keterbatasan sumber daya manusia bidang IT, dan disparitas infrastruktur antarrumah sakit. Hal ini mengakibatkan belum optimalnya implementasi standar perlindungan data di berbagai fasilitas layanan Kesehatan. Penegakan kebijakan akses minimal dalam sistem rumah sakit sangat penting. Setiap pengguna sistem informasi harus diberi hak akses sesuai tugasnya saja dan jejak akses (audit trail) wajib direkam untuk memudahkan investigasi jika terjadi insiden kebocoran data (Nadiroh & Wiraguna, 2025).

Persetujuan pasien dalam pengelolaan data tidak sekadar formalitas, melainkan proses edukasi yang mendalam mengenai hak dan risiko penggunaan data kesehatan mereka. Rumah sakit harus memberikan penjelasan ringkas dan mudah dipahami, serta tetap menghormati hak pasien jika ingin menarik persetujuan pengolahan data. Audit keamanan secara berkala perlu dilakukan untuk deteksi dini potensi celah keamanan. Audit mandiri atau eksternal juga membantu memastikan bahwa sistem dan kebijakan di rumah sakit berjalan efektif dan sesuai regulasi yang berlaku (*Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*, 2022, p. 27).

Sinergi lintas lembaga menjadi unsur penunjang keamanan data pasien. Kerja sama rumah sakit dengan Kementerian Kesehatan, BSSN, dan lembaga pengawas data diperlukan dalam penanganan insiden dan pembaruan kebijakan nasional di bidang kesehatan digital. Penguatan sistem keamanan siber rumah sakit wajib diiringi sosialisasi dan literasi digital bagi pasien. Kepercayaan masyarakat hanya dapat dibangun jika rumah sakit terbuka soal penggunaan dan perlindungan data, serta responsif terhadap keluhan dan aduan berkaitan dengan keamanan data pasien (Listianingrum et al., 2019).

Di era digital, peran rumah sakit sebagai pengendali data tidak sekadar administratif, tetapi juga strategis dalam menciptakan layanan kesehatan yang aman, terpercaya, dan patuh hukum. Upaya perlindungan data pasien yang konsisten akan memperkuat kepercayaan publik dan mendukung transformasi digital kesehatan yang berkelanjutan.

Tantangan Dan Strategi Pengendalian Data Pada Era Digital

Di era digital, revolusi teknologi telah mendorong transformasi mendalam pada sistem pengelolaan data di rumah sakit. Adaptasi pada sistem digital menjadi kebutuhan mutlak, namun turut menghadirkan tantangan kompleks yang harus dihadapi guna menjamin keamanan dan kerahasiaan data pasien. Salah satu tantangan utama adalah risiko kebocoran dan pencurian data pasien yang semakin meningkat sejalan dengan maraknya serangan siber, peretasan, hingga penjualan data di forum gelap. Nilai tinggi data medis dan identitas pasien menjadikan rumah sakit sasaran bagi pelaku kejahatan digital (Permana, 2024).

Kerentanan pada infrastruktur teknologi informasi rumah sakit juga menjadi hambatan signifikan. Perangkat keras yang usang, jaringan internet terbatas, dan kurangnya integrasi antar sistem menghambat upaya mempertahankan keamanan serta efisiensi data. Kurangnya pemahaman teknologi dan literasi digital, baik di kalangan tenaga medis maupun pasien, memperbesar peluang terjadinya pelanggaran protokol keamanan (Dewi, 2025). Banyak tenaga kesehatan yang belum terlatih menggunakan perangkat digital secara aman dan bertanggung jawab. Kepatuhan pada regulasi perlindungan data, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) dan Permenkes, juga belum sepenuhnya optimal. Audit terbaru bahkan menunjukkan 80% rumah sakit tidak sepenuhnya patuh pada peraturan ini, sehingga memperbesar risiko pelanggaran hukum dan privasi (Lestari, 2020).

Tantangan lain datang dari manajemen identitas digital. Kontrol dan validasi hak akses yang lemah, penggunaan akun bersama, dan lemahnya pengawasan aktivitas sistem memudahkan pelaku internal untuk melakukan penyalahgunaan data. Integrasi sistem informasi rumah sakit (SIMRS) dengan aplikasi eksternal seringkali mengakibatkan duplikasi dan inkonsistensi data (Sari & Wirman, 2021). Kompleksitas ini meningkatkan peluang terjadi human error maupun penyusupan melalui celah keamanan aplikasi pihak ketiga. Budaya keamanan data di lingkungan internal rumah

sakit umumnya masih lemah. Minimnya pelatihan rutin atau sosialisasi mengenai etika dan keamanan digital mendorong kasus kelalaian, yang kerap berujung pada insiden kebocoran data.

Sistem keamanan yang kurang responsif terhadap ancaman baru juga menjadi masalah. Banyak rumah sakit yang belum memperbarui firewall, sistem deteksi intrusi, dan perangkat lunak keamanan secara rutin. Strategi pengendalian data menyeluruh diawali dengan pembangunan infrastruktur teknologi informasi yang modern. Rumah sakit mesti menganggarkan pembaruan server, jaringan terenkripsi, serta backup data berbasis cloud yang andal (Utama, 2023).

Penerapan enkripsi end-to-end pada seluruh informasi medis, baik saat penyimpanan maupun transmisi, merupakan langkah efektif menutup akses pihak tidak berwenang. Hal ini dilengkapi dengan sistem autentikasi ganda atau berbasis biometrik untuk kontrol akses pengguna. Audit keamanan data dilakukan secara berkala guna mendeteksi dan menanggulangi potensi kelemahan sistem. Audit mencakup pengujian penetrasi, evaluasi kebijakan akses, serta simulasi insiden darurat untuk memastikan respons cepat dan tepat (Putri, 2023).

Sumber daya manusia menjadi ujung tombak lain dalam strategi pengendalian data. Rumah sakit wajib memberikan pelatihan rutin keamanan siber kepada tenaga medis, staf administrasi, dan semua pihak dengan akses ke sistem informasi pasien. Pembuatan dan penegakan standar operasional prosedur (SOP) terkait pengelolaan data sangat krusial. SOP ini mengatur klasifikasi kerahasiaan, alur akses, langkah identifikasi insiden, hingga sanksi atas pelanggaran yang terjadi (Farhan, 2023).

Strategi mitigasi risiko mencakup pembentukan tim tanggap darurat keamanan siber, penunjukan peran khusus Chief Information Security Officer (CISO), serta pengadaan sistem backup data yang siap pulih bila terjadi serangan. Kolaborasi dengan pihak ketiga, seperti vendor teknologi dan regulator, diperlukan dalam pembaruan protokol keamanan dan sertifikasi sistem. Standar keamanan internasional seperti ISO/IEC 27001 menjadi referensi penguatan tata kelola informasi (Komala Sari & Griadhi, 2024).

Terakhir, sosialisasi hak dan edukasi privasi bagi pasien harus digalakkan. Rumah sakit perlu menyediakan kanal pengaduan, informasi persetujuan pemrosesan data, dan transparansi atas penggunaan data medis.

Dengan demikian, tantangan yang semakin dinamis dan ancaman yang semakin beragam, strategi pengendalian data pada era digital harus berlapis, adaptif, dan didukung kemauan kolektif seluruh ekosistem rumah sakit untuk menjamin keamanan, privasi, dan kepercayaan masyarakat terhadap layanan kesehatan digital.

Kesimpulan

Rumah sakit memiliki peran yang sangat strategis sebagai pengendali data dalam memastikan keamanan data pribadi pasien di era sistem kesehatan digital. Mereka

berkewajiban menerapkan prosedur perlindungan data yang ketat, mematuhi regulasi seperti Undang-Undang Perlindungan Data Pribadi serta Permenkes, dan menjamin pelaksanaan kontrol akses, enkripsi, serta pencatatan seluruh aktivitas pemrosesan data. Tanggung jawab ini mencakup pengawasan internal dan eksternal agar hanya pihak yang berwenang yang dapat mengakses informasi sensitif pasien, sehingga potensi pelanggaran maupun kebocoran data dapat diminimalisir.

Meskipun berbagai upaya dan sistem keamanan sudah diterapkan, rumah sakit tetap menghadapi tantangan besar seperti ancaman serangan siber, minimnya literasi teknologi di kalangan tenaga kesehatan, ketertinggalan infrastruktur, hingga manajemen akses yang masih belum sempurna. Implementasi teknologi terbaru, audit keamanan secara berkala, serta pelatihan sumber daya manusia secara kontinu menjadi kunci penguatan perlindungan data pribadi pasien di tengah terus berkembangnya digitalisasi layanan kesehatan.

Dengan penguatan peran rumah sakit sebagai pengendali data, masyarakat dapat lebih percaya pada layanan kesehatan digital. Komitmen rumah sakit dalam melindungi privasi dan keamanan data pasien akan meningkatkan kualitas pelayanan, mendukung transformasi digital, sekaligus memastikan bahwa hak-hak pasien atas privasi data tetap terjaga dengan baik sesuai standar etika dan hukum di Indonesia.

References

- Algifari, M. H. (2024). Digital Health Literacy and Its Associated Factors in Indonesia. *Indonesian Journal of Public Health*, 15(2), 154–165. <https://doi.org/10.22146/ijph.5640>
- Annan, A. (2024). Tinjauan Yuridis Perlindungan Data Pribadi pada Sektor Kesehatan Berdasarkan UU No. 27 Tahun 2022. *Synergy: Jurnal Ilmiah Multidisiplin*, 1(4), 247–254.
- Bonsapia, M. & Jumiran. (2025). Aspek Hukum Telemedicine di Indonesia. *The Juris*, 9(1), 259–268. <https://doi.org/10.56301/juris.v9i1.1636>
- Dalimunthe, W. (2024). Patient Legal Protection in the Digital Era and Study of Indonesian Telemedicine Regulation. *Jurnal Hukum Kesehatan Indonesia*, 1(1), 1–10.
- Dewi, S. (2025). Perlindungan Hukum Bagi Pasien Konsultasi Online yang Mengalami Kerugian dalam Layanan Telemedicine di Indonesia. *Jurnal ISO: Jurnal Ilmu Sosial, Politik Dan Humaniora*, 5(1).
- Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, 3(2), Article 2.
- Farhan, N. (2023). A Literature Review of Telemedicine in Indonesia: Past, Present, and Future Prospective. *Jurnal Administrasi Kesehatan Indonesia*, 7(2).
- Ferrari, R. (2020). Writing narrative style literature reviews. *Medical Writing*, 24(4), 230–235. <https://doi.org/10.1179/2047480615Z.000000000329>
- Komala Sari, N. N. W. R., & Griadhi, N. M. A. Y. (2024). Analisis Pertanggungjawaban Hukum Penyedia Layanan Kesehatan (Telemedicine) Apabila Terjadi Kerugian

- Terhadap Pasien. Kertha Semaya, 12(5).
<https://doi.org/10.24843/KS.2024.v12.i05.p13>
- Lestari, H. (2020). *Hukum Jaminan Kesehatan Nasional*. Pustaka Pelajar.
- Listianingrum, D. M., Budiharto, & Mahmud, S. (2019). Perlindungan Hukum Terhadap Konsumen Dalam Pelayanan Kesehatan Berbasis Aplikasi Online. *Diponegoro Law Journal*.
- Nadiroh, A., & Wiraguna, S. A. (2025). Analisis Yuridis Kebocoran Data di Layanan Kesehatan Digital: Studi Kasus Aplikasi Telemedicine di Indonesia. *Media Hukum Indonesia*, 2(6), 313–320.
- Nurhayati, R. H. (2025). Legal Protection for Patients in Telemedic Services in Indonesia. *Journal of Legal, Public and Humanity*, 5(3). <https://doi.org/10.38035/jlph.v5i3.1592>
- Permana, A. (2024). Perlindungan Hukum Bagi Pasien Telemedicine Berdasarkan UU No. 17 Tahun 2023. *Jurnal Kesehatan Digital*, 1(2).
- Pramukars, D. T. (2021). Perlindungan Hukum bagi Pasien dalam Telemedicine. *Jurnal Cakrawala Informasi*, 1(2), 51–56.
- Purnama, S. (2024). Assessing Telemedicine Demand and Viability in Indonesian Geriatric Clinics: A Comprehensive HOT FIT and Sociotechnical Analysis. *Current Aging Science*, 18(1), 47–58. <https://doi.org/10.2174/0118746098302999240522092726>
- Putri, A. (2023). Implementasi Telemedicine di Indonesia: Problematika Hukum dan Perlindungan Data Pasien. *Jurnal Hukum & Kesehatan*, 8(1).
- Rahma, D., & Supriyadi, H. (2024). Telemedicine Regulation in Indonesia: Legal Frameworks, Challenges, and Future Directions. *Journal of Law and Technology*, 7(3), 213–230. <https://doi.org/10.33560/jmiki.v13i1.795>
- Rimbun, L. R., Marisi, E. L. D. D., & Hidayati, T. (2024). Tantangan Keamanan Data dalam Telemedicine: Implikasi terhadap Privasi Pasien dan Kepercayaan dalam Layanan Kesehatan Digital: Systematic Review. *Malahayati Health Student Journal*, 4(10).
- Sari, G., & Wirman, W. (2021). Perlindungan Data Pasien Telemedicine dalam Pandangan UU PDP. *Jurnal Komunikasi*, 15(1), 45.
- Syarifuddin, A. (2024). Indonesian Telemedicine: Between Hope and Legal Challenges. *Indonesian Journal of Humanities and Social Sciences*, 5(3), 1249–1258. <https://doi.org/10.33367/ijhass.v5i3.5936>
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. (2022).
- Utama, R. B. (2023). Patient Safety and Legal Certainty on Telemedicine Services in Indonesia. *Indonesian Journal of Health Law*, 4(2). <https://doi.org/10.32734/ijhl.v4i2.10624>
- Wahyudin, B. (2025). Legal Protection for Doctors in Telemedicine Services: Government Responsibility in Supporting SDGs 3 and 9 in Indonesia. *Journal of Lifestyle and SDGs Review*, 5(3). <https://doi.org/10.47172/2965-730X.SDGsReview.v5.n03.pe05139>
- Yuliana, D. (2021). *Tanggung Jawab Penyedia Layanan Kesehatan dalam Era Digitalisasi*.
- Yusriadi, -. (2025). Digital Transformation of Health Services in Indonesia Through the Utilization of AI, Big Data, and Telemedicine. 5(1), 85–93. <https://doi.org/10.62951/icistech.v5i1.270>