NETIZEN: JOURNAL OF SOCIETY AND BUSSINESS
Vol. 2 No. 12 November (2026), hal., 888-903
https://languar.net/index.php/NETIZEN
e-ISSN: 3032-4319

PERLINDUNGAN HUKUM DATA PRIBADI PASIEN DALAM DIGITALISASI PELAYANAN KESEHATAN DI INDONESIA: KAJIAN PUSTAKA

Gunawan Widjaja
Fakultas Hukum Universitas 17 Agustus 1945 Jakarta
widjaja_gunawan@yahoo.com

Hotmaria Hertawaty Sijabat
Gunawan Widjaja Learning Centre
sijabathotmaria@gmail.com

Abstract

The digitalisation of healthcare services in Indonesia through the use of electronic health records, telemedicine, health applications and data exchange between healthcare facilities offers benefits in terms of improving the efficiency, accessibility, speed and quality of services. However, digitalisation also poses risks to the security and confidentiality of patients' personal data, such as data breaches, unauthorised access, misuse of medical information and cyber-attacks. This study aims to analyse the legal framework for the protection of patients' personal data, as well as the challenges and strategies for strengthening it within the digitalisation of healthcare services in Indonesia. The study employs a literature review using a normative legal approach and descriptive-qualitative analysis. The findings indicate that the protection of patients' personal data has a legal basis in Law No. 27 of 2022 on the Protection of Personal Data, Law No. 17 of 2023 on Health, and Minister of Health Regulation No. 24 of 2022 on Medical Records. Health data constitutes specific personal data and therefore requires a higher level of protection. Nevertheless, its implementation still faces challenges in the form of regulatory fragmentation, infrastructure limitations, low digital literacy, cyber security threats, weak access controls, and unclear third-party responsibilities. Therefore, there is a need to strengthen data governance, implement multi-layered technological security, enhance the competence of human resources, ensure transparency in data processing, and establish effective oversight and law enforcement. The protection of patient data must be an integral part of the development of digital healthcare services that are secure, trustworthy and patient-rights-oriented.

Keywords: *legal protection, patient personal data, healthcare digitalisation, electronic medical records, data security.*

Abstrak

Digitalisasi pelayanan kesehatan di Indonesia melalui penggunaan Rekam Medis Elektronik, telemedicine, aplikasi kesehatan, dan pertukaran data antar fasilitas pelayanan kesehatan memberikan manfaat dalam meningkatkan efisiensi, aksesibilitas, kecepatan, dan kualitas pelayanan. Namun, digitalisasi juga menimbulkan risiko terhadap keamanan dan kerahasiaan data pribadi pasien, seperti kebocoran data, akses tanpa kewenangan, penyalahgunaan informasi medis, dan serangan siber. Penelitian ini bertujuan menganalisis kerangka hukum perlindungan data pribadi pasien serta tantangan dan strategi penguatannya dalam digitalisasi pelayanan kesehatan di Indonesia. Penelitian ini menggunakan metode kajian pustaka dengan pendekatan yuridis normatif dan analisis

deskriptif-kualitatif. Hasil kajian menunjukkan bahwa perlindungan data pribadi pasien memiliki dasar hukum melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, dan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. Data kesehatan termasuk data pribadi spesifik sehingga memerlukan perlindungan yang lebih tinggi. Meskipun demikian, penerapannya masih menghadapi tantangan berupa fragmentasi regulasi, keterbatasan infrastruktur, rendahnya literasi digital, ancaman keamanan siber, lemahnya pengendalian akses, dan ketidakjelasan tanggung jawab pihak ketiga. Oleh karena itu, diperlukan penguatan tata kelola data, penerapan keamanan teknologi berlapis, peningkatan kompetensi sumber daya manusia, transparansi pemrosesan data, serta pengawasan dan penegakan hukum yang efektif. Perlindungan data pasien harus menjadi bagian integral dari pembangunan pelayanan kesehatan digital yang aman, terpercaya, dan berorientasi pada hak pasien.
Kata kunci: perlindungan hukum, data pribadi pasien, digitalisasi kesehatan, rekam medis elektronik, keamanan data.

Pendahuluan

Transformasi digital telah mengubah pola penyelenggaraan pelayanan kesehatan di Indonesia. Pemanfaatan teknologi informasi kini terlihat dalam penggunaan rekam medis elektronik, pendaftaran pasien secara daring, telemedicine, resep elektronik, aplikasi kesehatan, sistem informasi rumah sakit, serta pertukaran data kesehatan antar fasilitas pelayanan Kesehatan (Zhang dkk., 2024). Digitalisasi tersebut diharapkan mampu meningkatkan efisiensi administrasi, mempercepat akses pelayanan, mendukung ketepatan diagnosis, dan memperkuat kesinambungan perawatan pasien. Organisasi Kesehatan Dunia menempatkan kesehatan digital sebagai instrumen penting untuk meningkatkan akses, mutu, efisiensi, dan keberlanjutan pelayanan kesehatan. Dalam konteks Indonesia, strategi transformasi kesehatan digital diarahkan untuk mengatasi fragmentasi data kesehatan, memperkuat interoperabilitas sistem, serta mengembangkan platform terintegrasi yang mampu menghubungkan berbagai fasilitas pelayanan kesehatan (World Health Organization [WHO], 2021, 2024).

Penggunaan teknologi digital dalam pelayanan kesehatan juga berkaitan dengan perubahan cara data pasien dikumpulkan, disimpan, dipertukarkan, dan dianalisis. Pada sistem konvensional, informasi pasien umumnya tersimpan dalam bentuk dokumen fisik yang aksesnya relatif terbatas pada fasilitas kesehatan tertentu. Sebaliknya, sistem digital memungkinkan data kesehatan diakses secara cepat oleh berbagai pihak melalui jaringan elektronik (Yandi dkk., 2025). Perubahan ini memberikan manfaat besar bagi kesinambungan pelayanan, terutama ketika pasien memperoleh layanan dari lebih dari satu fasilitas kesehatan. Namun, kemudahan akses tersebut sekaligus memperluas kemungkinan terjadinya akses tanpa kewenangan, perubahan data, penyalahgunaan informasi, maupun kebocoran data. Dengan demikian, digitalisasi pelayanan kesehatan tidak cukup hanya dinilai dari aspek efisiensi teknologi, tetapi juga harus dilihat dari aspek keamanan, kerahasiaan, akuntabilitas, dan perlindungan hak pasien (Wiley & Gostin, 2025).

Data kesehatan pasien merupakan salah satu jenis data yang memiliki tingkat sensitivitas tinggi. Data tersebut tidak hanya mencakup nama dan identitas pasien, tetapi juga diagnosis, riwayat penyakit, hasil pemeriksaan laboratorium, tindakan medis, penggunaan obat, kondisi psikologis, informasi reproduksi, data biometrik, dan informasi genetik. Apabila informasi tersebut tersebar atau digunakan secara tidak sah, pasien dapat mengalami berbagai bentuk kerugian, seperti diskriminasi, stigma sosial, pemerasan, penolakan asuransi, kerugian ekonomi, dan gangguan terhadap kehidupan pribadi (Widyawati dkk., 2025). WHO menegaskan bahwa data kesehatan perlu diperlakukan sebagai data pribadi sensitif yang harus dilindungi melalui dasar hukum yang jelas, transparansi pemrosesan, mekanisme persetujuan, pengendalian akses, audit, serta langkah keamanan terhadap pemrosesan yang tidak sah (WHO, 2021).

Dalam hukum Indonesia, data kesehatan telah ditempatkan sebagai data pribadi yang bersifat spesifik. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menyebutkan bahwa data dan informasi kesehatan termasuk dalam kategori data pribadi spesifik. Penggolongan tersebut menunjukkan bahwa pemrosesan data kesehatan memerlukan perlindungan yang lebih ketat dibandingkan data pribadi umum karena dampak pelanggarannya dapat lebih serius bagi subjek data. UU PDP juga mengatur hak subjek data pribadi, dasar pemrosesan data, kewajiban pengendali dan prosesor data, keamanan pemrosesan, pemberitahuan kegagalan perlindungan data, serta sanksi terhadap pelanggaran. Oleh karena itu, pengelolaan data pasien dalam sistem kesehatan digital harus dilaksanakan berdasarkan prinsip keabsahan, transparansi, pembatasan tujuan, akurasi, keamanan, dan pertanggungjawaban (Republik Indonesia, 2022a).

Perlindungan hukum terhadap data pasien juga memiliki keterkaitan erat dengan pengaturan rekam medis. Rekam medis bukan sekadar dokumen administratif, melainkan dokumen yang memuat informasi penting mengenai identitas, kondisi kesehatan, pemeriksaan, diagnosis, pengobatan, dan tindakan medis yang diterima pasien. Dalam konteks digitalisasi, rekam medis mengalami perubahan bentuk dari dokumen konvensional menjadi Rekam Medis Elektronik yang dapat dibuat, disimpan, diakses, dan dipertukarkan melalui sistem elektronik. Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis mengatur penyelenggaraan rekam medis, termasuk kewajiban memperhatikan prinsip keamanan dan kerahasiaan data serta informasi. Ketentuan tersebut menegaskan bahwa pemanfaatan teknologi dalam rekam medis harus disertai pengendalian akses dan perlindungan terhadap integritas informasi pasien (Kementerian Kesehatan Republik Indonesia, 2022).

Penyelenggaraan Rekam Medis Elektronik juga didukung oleh Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan yang mengakui pemanfaatan teknologi dalam penyelenggaraan pelayanan kesehatan. Teknologi dapat digunakan untuk mendukung pelayanan informasi kesehatan, layanan mandiri, telekesehatan, dan telemedicine. Meskipun demikian, pemanfaatan teknologi dalam pelayanan kesehatan harus tetap memperhatikan hak pasien dan prinsip kerahasiaan informasi medis. Artinya, peningkatan akses terhadap data kesehatan tidak dapat dimaknai sebagai kebebasan bagi setiap pihak

untuk membuka atau menggunakan informasi pasien. Akses harus diberikan berdasarkan kewenangan, tujuan pelayanan, kebutuhan profesional, serta ketentuan hukum yang berlaku (Republik Indonesia, 2023).

Dalam sistem pelayanan kesehatan digital, tanggung jawab perlindungan data tidak hanya berada pada dokter atau tenaga kesehatan yang berhubungan langsung dengan pasien. Rumah sakit, klinik, puskesmas, laboratorium, apotek, perusahaan teknologi kesehatan, penyedia layanan cloud, dan pihak pengelola sistem informasi juga dapat terlibat dalam pemrosesan data pasien. Pihak-pihak tersebut dapat berkedudukan sebagai pengendali atau prosesor data, bergantung pada kewenangan dan tujuan pemrosesan yang dilakukannya. Penelitian mengenai tanggung jawab rumah sakit menunjukkan bahwa rumah sakit dapat memiliki tanggung jawab sebagai pengendali data pribadi sekaligus penyelenggara sistem elektronik. Apabila terjadi penyalahgunaan data pasien, rumah sakit berpotensi menghadapi tanggung jawab administratif, perdata, maupun pidana sesuai dengan bentuk pelanggaran yang terjadi (Lukitasari dkk., 2023).

Tantangan perlindungan data pasien semakin kompleks karena sistem kesehatan digital menghadapi berbagai ancaman keamanan siber. Ancaman tersebut dapat berupa pencurian kata sandi, phishing, malware, ransomware, peretasan basis data, kesalahan konfigurasi sistem, penggunaan perangkat yang tidak aman, serta akses internal yang melampaui kewenangan. Selain serangan dari pihak luar, kelalaian manusia juga dapat menjadi penyebab kebocoran data, misalnya pengiriman dokumen kepada penerima yang salah, penggunaan akun secara bersama-sama, atau tidak adanya pembatasan hak akses. Penelitian mengenai penerapan rekam medis elektronik di Indonesia menunjukkan bahwa proses digitalisasi masih menghadapi perbedaan infrastruktur, keterbatasan konektivitas internet, rendahnya literasi digital tenaga kesehatan, dan masih digunakannya dokumen kertas secara bersamaan pada masa transisi (Syadina dkk., 2025).

Persoalan perlindungan data pasien juga berkaitan dengan kesiapan kelembagaan dan harmonisasi regulasi. Meskipun Indonesia telah memiliki UU PDP, UU Kesehatan, Permenkes tentang Rekam Medis, serta berbagai aturan mengenai sistem elektronik, pelaksanaannya masih memerlukan sinkronisasi. Beberapa isu yang perlu diperjelas antara lain kedudukan pengendali data, hak pasien atas rekam medis, batas kewenangan tenaga kesehatan, pemrosesan data untuk penelitian, penggunaan penyedia teknologi pihak ketiga, mekanisme pelaporan insiden, serta bentuk tanggung jawab ketika terjadi kebocoran data. Kajian mengenai perlindungan hukum rekam medis pasien di Indonesia menunjukkan bahwa ketidakharmonisan antarregulasi dapat menimbulkan ketidakpastian hukum mengenai pihak yang bertanggung jawab, mekanisme perlindungan, dan penerapan sanksi (Takaryanto & Lany, 2025).

Selain aspek regulasi dan teknologi, perlindungan data pasien juga dipengaruhi oleh tingkat pemahaman pasien dan tenaga kesehatan. Pasien perlu mengetahui jenis data yang dikumpulkan, tujuan pemrosesan, pihak yang dapat mengakses, jangka waktu penyimpanan, dan hak yang dapat digunakan apabila terjadi pelanggaran. Di sisi lain, tenaga kesehatan dan pengelola sistem harus memahami bahwa kerahasiaan data pasien

merupakan kewajiban hukum dan etika profesi. Penelitian mengenai kesiapan fasilitas kesehatan di Indonesia menunjukkan bahwa perlindungan data pasien membutuhkan mekanisme berlapis yang mencakup kebijakan internal, pembagian tanggung jawab, pengendalian akses, pelatihan sumber daya manusia, serta pengawasan institusional (Siregar & Astuti, 2025).

Berdasarkan uraian tersebut, perlindungan hukum data pribadi pasien dalam digitalisasi pelayanan kesehatan merupakan persoalan yang penting untuk dikaji secara akademik dan praktis. Digitalisasi memang dapat meningkatkan mutu serta akses pelayanan, tetapi tanpa kerangka perlindungan yang memadai, teknologi juga dapat memperbesar risiko pelanggaran privasi dan penyalahgunaan data. Oleh karena itu, kajian ini bertujuan menganalisis kerangka hukum perlindungan data pribadi pasien dalam digitalisasi pelayanan kesehatan di Indonesia serta mengidentifikasi tantangan dan strategi penguatan implementasinya.

Metode Penelitian

Penelitian ini menggunakan metode kajian pustaka dengan pendekatan yuridis normatif dan analisis deskriptif-kualitatif (Eliyah & Aslan, 2025). Data penelitian diperoleh melalui penelusuran dan telaah terhadap sumber hukum primer, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, serta Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis, dan sumber hukum sekunder berupa buku, jurnal nasional dan internasional, dan dokumen lainnya yang terkait (Walliman & Walliman, 2021). Data yang terkumpul dianalisis dengan cara mengidentifikasi, mengklasifikasikan, membandingkan, dan menginterpretasikan ketentuan hukum serta hasil penelitian terdahulu untuk memperoleh gambaran mengenai kerangka hukum, tanggung jawab fasilitas pelayanan kesehatan, tantangan implementasi, dan strategi penguatan perlindungan data pribadi pasien di Indonesia.

Hasil dan Pembahasan

Kerangka Hukum Perlindungan Data Pribadi Pasien dalam Digitalisasi Pelayanan Kesehatan

Data pribadi pasien dalam pelayanan kesehatan digital memiliki kedudukan hukum yang penting karena berkaitan langsung dengan hak privasi, keamanan, dan martabat manusia. Data tersebut meliputi identitas pasien, riwayat penyakit, hasil pemeriksaan, diagnosis, tindakan medis, resep, kondisi psikologis, informasi reproduksi, data biometrik, dan informasi genetik. Karakteristik data kesehatan yang sensitif menyebabkan pengelolaannya tidak dapat disamakan dengan data administratif biasa (Xiaying, 2019). Kebocoran atau penggunaan data kesehatan tanpa kewenangan dapat menimbulkan kerugian sosial, ekonomi, psikologis, bahkan diskriminasi terhadap pasien. Oleh karena itu, perlindungan hukum data pasien harus mencakup pengaturan mengenai pengumpulan, penggunaan, penyimpanan, pertukaran, penghapusan, dan pemusnahan data secara

menyeluruh (Versaci, 2018). Dalam kerangka hukum Indonesia, perlindungan tersebut terutama bertumpu pada Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, serta Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis (Republik Indonesia, 2022a, 2023; Kementerian Kesehatan Republik Indonesia, 2022).

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi merupakan dasar hukum umum dalam pengelolaan data pribadi di Indonesia. Undang-undang tersebut membedakan data pribadi menjadi data pribadi umum dan data pribadi spesifik. Data dan informasi kesehatan termasuk dalam kategori data pribadi spesifik bersama dengan data biometrik, data genetika, catatan kejahatan, data anak, dan data keuangan pribadi (Ventura & Coeli, 2018). Penggolongan data kesehatan sebagai data pribadi spesifik menunjukkan bahwa negara mengakui adanya risiko yang lebih besar apabila data tersebut diproses secara tidak sah. Dalam konteks pelayanan kesehatan digital, ketentuan ini berlaku terhadap data yang diproses oleh rumah sakit, klinik, puskesmas, laboratorium, apotek, aplikasi kesehatan, penyedia telemedicine, maupun penyedia layanan teknologi informasi yang mengelola data pasien. Dengan demikian, setiap pemrosesan data pasien harus memiliki dasar hukum, tujuan yang jelas, serta mekanisme keamanan yang sesuai dengan tingkat sensitivitas data tersebut (Republik Indonesia, 2022a).

UU PDP memberikan sejumlah hak kepada pasien sebagai subjek data pribadi. Pasien berhak memperoleh informasi mengenai identitas pihak yang memproses data, dasar kepentingan hukum, tujuan pemrosesan, serta pertanggungjawaban pihak yang meminta data. Pasien juga memiliki hak untuk melengkapi, memperbarui, dan memperbaiki data yang tidak akurat, serta memperoleh akses dan salinan data pribadi mengenai dirinya (Takaryanto & Lany, 2025). Dalam konteks rekam medis elektronik, hak tersebut berarti pasien memiliki kepentingan hukum untuk mengetahui informasi yang tersimpan mengenai dirinya dan memastikan bahwa informasi tersebut benar serta tidak menimbulkan kesalahan dalam pelayanan. Pasien juga dapat menggunakan atau mengirimkan datanya kepada pengendali data lain sepanjang sistem yang digunakan mampu berkomunikasi secara aman. Pengakuan terhadap hak-hak tersebut memperkuat posisi pasien, yang sebelumnya cenderung berada dalam posisi yang lebih lemah dibandingkan fasilitas pelayanan kesehatan (Republik Indonesia, 2022a; Kementerian Komunikasi dan Informatika Republik Indonesia, 2022).

Perlindungan data pasien juga mensyaratkan adanya dasar pemrosesan data yang sah. Fasilitas pelayanan kesehatan tidak boleh mengumpulkan atau menggunakan data pasien tanpa tujuan yang dapat dibenarkan secara hukum. Pemrosesan dapat dilakukan berdasarkan persetujuan pasien, kewajiban hukum, pelaksanaan pelayanan kesehatan, perlindungan kepentingan vital, kepentingan publik, atau dasar hukum lain yang diakui oleh UU PDP (Siregar & Astuti, 2025). Dalam pelayanan medis, tidak semua pemrosesan harus selalu didasarkan pada persetujuan tertulis karena terdapat tindakan yang memang diperlukan untuk memenuhi kewajiban pelayanan dan keselamatan pasien. Namun,

penggunaan data di luar tujuan pelayanan, seperti untuk promosi, penelitian, analisis komersial, atau pemberian kepada pihak ketiga, harus memiliki dasar pemrosesan yang sesuai. Persetujuan yang diberikan pasien juga harus bersifat jelas, spesifik, diberikan secara sadar, dan tidak diperoleh melalui informasi yang menyesatkan (Republik Indonesia, 2022a).

UU PDP juga menetapkan kewajiban pengendali data pribadi untuk memproses data secara terbatas, spesifik, sah secara hukum, dan transparan. Dalam konteks pelayanan kesehatan, rumah sakit atau fasilitas kesehatan pada umumnya memiliki peran sebagai pengendali data karena menentukan tujuan dan cara pemrosesan data pasien. Pengendali wajib memastikan bahwa data yang dikumpulkan sesuai dengan kebutuhan pelayanan, tidak berlebihan, akurat, lengkap, dan relevan (Santo dkk., 2024). Pengendali juga wajib melakukan pencatatan terhadap kegiatan pemrosesan, menjaga kerahasiaan, mengawasi pihak-pihak yang terlibat, serta memastikan keamanan data dari gangguan, kehilangan, penyalahgunaan, dan akses tanpa kewenangan. Kewajiban tersebut memperlihatkan bahwa perlindungan data tidak berhenti pada saat data dikumpulkan, tetapi berlaku sepanjang siklus hidup data, mulai dari penciptaan hingga pemusnahan (Republik Indonesia, 2022a; Kementerian Komunikasi dan Informatika Republik Indonesia, 2022).

Dalam digitalisasi pelayanan kesehatan, pengendali data sering kali bekerja sama dengan prosesor data. Prosesor dapat berupa penyedia perangkat lunak rumah sakit, perusahaan pengembang aplikasi kesehatan, penyedia penyimpanan cloud, penyedia layanan pusat data, atau perusahaan yang membantu pemeliharaan sistem. Hubungan antara pengendali dan prosesor harus diatur secara jelas melalui perjanjian yang memuat tujuan pemrosesan, jenis data, jangka waktu penyimpanan, batas kewenangan akses, standar keamanan, serta mekanisme penanganan insiden (Salijeni dkk., 2018). Meskipun data diproses oleh pihak ketiga, fasilitas pelayanan kesehatan tidak dapat sepenuhnya melepaskan tanggung jawabnya kepada vendor. Fasilitas kesehatan tetap berkewajiban melakukan pengawasan dan memastikan bahwa pihak ketiga memproses data sesuai dengan instruksi, perjanjian, serta peraturan perundang-undangan yang berlaku. Hal ini penting karena penggunaan layanan teknologi pihak ketiga dapat memperluas titik kerentanan dalam sistem pelayanan Kesehatan (Rinjani & Firmansyah, 2025).

Selain UU PDP, perlindungan data pasien diperkuat oleh Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan. Undang-undang ini mengatur penyelenggaraan kesehatan secara luas, termasuk pemanfaatan teknologi dalam pelayanan kesehatan, layanan informasi kesehatan, telekesehatan, dan telemedicine. Pemanfaatan teknologi tersebut harus dilaksanakan dengan tetap memperhatikan keamanan, kerahasiaan, mutu pelayanan, dan hak pasien (Putri & Putra, 2024). UU Kesehatan juga menempatkan rekam medis sebagai bagian penting dari dokumentasi pelayanan kesehatan. Oleh sebab itu, setiap proses digitalisasi pelayanan harus memastikan bahwa data yang dihasilkan, disimpan, dan dipertukarkan tetap dapat dipertanggungjawabkan secara medis dan

hukum. Integrasi teknologi tidak boleh mengurangi hak pasien atas kerahasiaan maupun meningkatkan risiko penggunaan data di luar tujuan pelayanan (Republik Indonesia, 2023).

Pengaturan yang lebih teknis mengenai rekam medis terdapat dalam Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. Peraturan ini mewajibkan fasilitas pelayanan kesehatan menyelenggarakan Rekam Medis Elektronik sebagai bagian dari proses pelayanan. Rekam Medis Elektronik harus diselenggarakan dengan memperhatikan prinsip keamanan dan kerahasiaan data serta informasi. Prinsip keamanan tersebut mencakup kerahasiaan, integritas, dan ketersediaan data. Kerahasiaan berarti data hanya dapat diakses oleh pihak yang memiliki kewenangan; integritas berarti data harus tetap utuh, akurat, dan tidak diubah secara tidak sah; sedangkan ketersediaan berarti data dapat diakses ketika diperlukan untuk kepentingan pelayanan. Kementerian Kesehatan juga menegaskan bahwa pasien berhak memperoleh isi rekam medisnya dan pemberian akses kepada pihak lain harus memperhatikan persetujuan pasien serta ketentuan hukum yang berlaku (Kementerian Kesehatan Republik Indonesia, 2022; Kementerian Kesehatan Republik Indonesia, 2022b).

Kerahasiaan rekam medis memiliki hubungan erat dengan kewajiban etika dan profesional tenaga kesehatan. Semua pihak yang terlibat dalam pelayanan kesehatan wajib menjaga kerahasiaan isi rekam medis, termasuk setelah pasien meninggal dunia. Dalam sistem digital, kewajiban tersebut diterapkan melalui pembatasan hak akses, penggunaan akun individual, autentikasi pengguna, pencatatan aktivitas, dan pengawasan terhadap siapa saja yang membuka data pasien (Nugroho dkk., 2024). Tenaga kesehatan hanya boleh mengakses informasi yang relevan dengan tugas dan kebutuhan pelayanan. Staf administrasi, tenaga teknis, dan pihak pengelola sistem juga tidak boleh membuka atau menyebarluaskan data pasien tanpa alasan yang sah. Dengan demikian, kerahasiaan pasien tidak hanya bergantung pada perilaku dokter atau perawat, tetapi juga pada desain sistem, kebijakan internal, budaya organisasi, dan pengawasan fasilitas pelayanan Kesehatan (Nocker & Sena, 2019).

Perlindungan hukum terhadap data pasien juga mencakup aspek keamanan teknis dan organisasi. Fasilitas pelayanan kesehatan perlu menerapkan pengamanan berlapis, seperti enkripsi, autentikasi multifaktor, pengendalian akses berbasis peran, pencadangan data, pemantauan aktivitas, pengujian keamanan, pembaruan perangkat lunak, serta rencana pemulihan apabila terjadi gangguan. Pengamanan organisasi dapat dilakukan melalui penyusunan kebijakan perlindungan data, penunjukan pihak yang bertanggung jawab, pelatihan tenaga kesehatan, audit berkala, dan prosedur penanganan insiden. Kewajiban ini sejalan dengan UU PDP yang mengharuskan pengendali menentukan tingkat keamanan berdasarkan sifat dan risiko data yang diproses. Karena data kesehatan termasuk data pribadi spesifik, standar pengamanannya harus lebih tinggi daripada data yang memiliki tingkat sensitivitas rendah (Republik Indonesia, 2022a; Kementerian Komunikasi dan Informatika Republik Indonesia, 2022).

Dengan demikian, kerangka hukum perlindungan data pribadi pasien pada akhirnya harus dipahami sebagai satu kesatuan antara UU PDP sebagai aturan umum, UU

Kesehatan sebagai aturan sektoral, dan Permenkes tentang Rekam Medis sebagai aturan teknis. UU PDP memberikan prinsip, hak, kewajiban, serta sanksi dalam pemrosesan data pribadi; UU Kesehatan memberikan dasar penyelenggaraan pelayanan kesehatan dan pemanfaatan teknologi; sedangkan Permenkes Nomor 24 Tahun 2022 memberikan ketentuan operasional mengenai rekam medis elektronik. Ketiga instrumen tersebut membentuk landasan hukum bagi perlindungan data pasien, meskipun masih diperlukan harmonisasi, pedoman teknis, pengawasan, serta peningkatan kapasitas fasilitas kesehatan. Dengan kerangka tersebut, perlindungan pasien tidak hanya dipahami sebagai kewajiban menjaga rahasia medis, tetapi juga sebagai kewajiban untuk menjamin transparansi, kontrol pasien, keamanan sistem, akurasi data, dan pertanggungjawaban setiap pihak yang memproses data pasien.

Tantangan dan Strategi Penguatan Perlindungan Data Pasien dalam Digitalisasi Kesehatan

Digitalisasi kesehatan di Indonesia memberikan manfaat besar bagi peningkatan kualitas, efisiensi, dan akses pelayanan kesehatan, tetapi juga menghadirkan tantangan serius dalam perlindungan data pasien. Penggunaan Rekam Medis Elektronik, telemedicine, aplikasi kesehatan, dan integrasi data melalui platform digital menyebabkan informasi pasien dapat dikumpulkan, disimpan, dan dipertukarkan secara lebih cepat (Riyantori & Buka, 2025). Di sisi lain, semakin banyak sistem dan pihak yang terlibat, semakin besar pula kemungkinan terjadinya akses tanpa kewenangan, kebocoran data, manipulasi informasi, dan penyalahgunaan data. Data kesehatan memiliki karakteristik sensitif sehingga membutuhkan perlindungan khusus, baik melalui kebijakan hukum maupun pengamanan teknis. Organisasi Kesehatan Dunia menekankan bahwa pengelolaan data kesehatan harus memperhatikan prinsip kerahasiaan, integritas, ketersediaan, transparansi, persetujuan, dan akuntabilitas (World Health Organization [WHO], 2021, 2024).

Tantangan pertama adalah adanya kesenjangan antara perkembangan regulasi dan penerapannya di lapangan. Indonesia telah memiliki Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis, serta berbagai regulasi mengenai penyelenggaraan sistem elektronik. Meskipun demikian, keberadaan regulasi belum sepenuhnya menjamin terlaksananya perlindungan data pasien secara konsisten. Sejumlah penelitian menunjukkan bahwa masalah utama bukan hanya kekurangan aturan, melainkan lemahnya penerapan, pengawasan, koordinasi, dan penegakan hukum. Kajian mengenai pertukaran Rekam Medis Elektronik bahkan menunjukkan adanya tumpang tindih kewenangan dan belum seragamnya prosedur terkait pembuktian serta penyelesaian sengketa kebocoran data medis (Yu & Zhao, 2019).

Tantangan kedua berkaitan dengan ketimpangan infrastruktur digital antara fasilitas pelayanan kesehatan. Rumah sakit besar di wilayah perkotaan umumnya memiliki sumber daya teknologi, tenaga ahli, dan anggaran yang lebih memadai dibandingkan klinik

kecil, praktik mandiri, atau puskesmas di daerah terpencil. Sebaliknya, sebagian fasilitas kesehatan masih menghadapi keterbatasan jaringan internet, perangkat keras, kapasitas penyimpanan, sistem pencadangan, serta tenaga teknologi informasi. Penelitian mengenai keamanan Rekam Medis Elektronik di Indonesia menunjukkan bahwa klinik kecil dan praktik mandiri sering mengalami kesulitan memenuhi standar keamanan yang dipersyaratkan karena keterbatasan teknis dan finansial. Kondisi tersebut dapat menimbulkan ketidakseimbangan perlindungan data pasien dan meningkatkan risiko kebocoran pada fasilitas kesehatan yang memiliki sistem keamanan paling lemah (Lestari dkk., 2024).

Tantangan ketiga adalah ancaman keamanan siber yang terus berkembang. Data pasien dapat menjadi sasaran pencurian melalui phishing, malware, ransomware, peretasan sistem, pencurian kata sandi, atau eksploitasi kelemahan perangkat lunak. Serangan terhadap sistem kesehatan dapat mengakibatkan dua jenis kerugian sekaligus, yaitu terganggunya pelayanan medis dan terbukanya informasi pribadi pasien. Apabila sistem Rekam Medis Elektronik tidak dapat diakses, tenaga kesehatan dapat mengalami kesulitan memperoleh riwayat penyakit atau hasil pemeriksaan yang diperlukan dalam keadaan mendesak. Sebaliknya, apabila basis data berhasil dicuri, informasi pasien dapat diperjualbelikan atau digunakan untuk pemerasan dan penipuan. Oleh karena itu, keamanan data pasien harus dipandang sebagai bagian dari keselamatan pasien, bukan hanya sebagai persoalan teknis teknologi informasi (UNICEF, 2024; WHO, 2021).

Tantangan keempat berkaitan dengan pengendalian akses terhadap data pasien. Dalam sistem digital, data pasien dapat diakses oleh dokter, perawat, tenaga administrasi, petugas laboratorium, apoteker, pengelola sistem, vendor teknologi, dan pihak lain yang terhubung dengan sistem. Apabila hak akses tidak dibatasi berdasarkan peran dan kebutuhan pekerjaan, terdapat risiko bahwa seseorang dapat melihat atau menyalin data pasien tanpa alasan yang sah. Penggunaan akun secara bersama-sama, kata sandi yang lemah, tidak adanya autentikasi multifaktor, dan tidak tersedianya pencatatan aktivitas pengguna dapat menyulitkan fasilitas kesehatan dalam mengetahui pihak yang bertanggung jawab atas akses tidak sah. Karena itu, diperlukan prinsip *least privilege* dan *need to know*, yaitu setiap pengguna hanya memperoleh akses minimum yang diperlukan untuk melaksanakan tugasnya (Angraeni dkk., 2026).

Tantangan kelima adalah rendahnya literasi digital dan pemahaman hukum di kalangan tenaga kesehatan maupun pasien. Sebagian tenaga kesehatan belum memperoleh pelatihan yang memadai mengenai keamanan kata sandi, pengenalan phishing, penggunaan perangkat pribadi, pengiriman dokumen medis, serta kewajiban menjaga kerahasiaan data pasien. Pada sisi lain, pasien belum tentu memahami bagaimana datanya dikumpulkan, untuk tujuan apa digunakan, berapa lama disimpan, dan kepada siapa dapat dibagikan. Rendahnya literasi tersebut dapat menyebabkan persetujuan diberikan tanpa pemahaman yang cukup dan meningkatkan kemungkinan kesalahan manusia. Penelitian mengenai penerapan Rekam Medis Elektronik di Indonesia juga menemukan bahwa penerapan sistem digital masih menghadapi hambatan berupa

keterbatasan kemampuan sumber daya manusia, resistensi pengguna, dan perbedaan kesiapan organisasi (Safitri Rahmadaniah & Harmanto, 2024).

Tantangan keenam muncul dari penggunaan pihak ketiga dan layanan komputasi awan. Banyak fasilitas kesehatan bekerja sama dengan perusahaan pengembang aplikasi, penyedia sistem informasi rumah sakit, penyedia pusat data, dan penyedia cloud untuk menyimpan atau mengelola data pasien (Udiana & Pramana, 2025). Kerja sama tersebut dapat meningkatkan efisiensi, tetapi juga menimbulkan risiko apabila kontrak tidak menjelaskan batas akses, lokasi penyimpanan, jangka waktu retensi, kewajiban keamanan, serta prosedur apabila terjadi insiden. Fasilitas kesehatan juga perlu mengetahui apakah vendor menggunakan subkontraktor dan apakah data pasien ditransfer ke pihak lain. Tanpa mekanisme uji kelayakan, audit, dan pengawasan, rumah sakit dapat kehilangan kendali atas data pasien meskipun secara hukum tetap memiliki tanggung jawab sebagai pengendali data (Takaryanto & Lany, 2025).

Tantangan ketujuh berkaitan dengan interoperabilitas dan pertukaran data antar sistem. Integrasi data kesehatan diperlukan agar informasi pasien dapat digunakan secara berkesinambungan oleh fasilitas yang berwenang. Namun, pertukaran data juga meningkatkan jumlah titik akses dan pihak yang terlibat dalam pemrosesan. Apabila standar autentikasi, enkripsi, format data, dan pencatatan aktivitas tidak seragam, proses integrasi dapat menimbulkan kerentanan baru. Selain itu, terdapat persoalan mengenai batas informasi yang boleh dibagikan, persetujuan pasien, hak akses lembaga pemerintah, serta penggunaan data untuk penelitian dan kebijakan publik. Karena itu, interoperabilitas harus dibangun secara aman dan berbasis tujuan, bukan sekadar menghubungkan semua data tanpa pembatasan (Susilo dkk., 2025).

Strategi pertama untuk memperkuat perlindungan data pasien adalah membangun tata kelola data yang jelas dan terintegrasi. Fasilitas kesehatan perlu menetapkan siapa yang bertindak sebagai pengendali data, siapa yang menjadi prosesor, jenis data yang diproses, tujuan pemrosesan, masa penyimpanan, serta pihak yang dapat memperoleh akses. Kebijakan internal harus memuat prosedur pendaftaran pasien, penggunaan Rekam Medis Elektronik, pemberian akses kepada tenaga kesehatan, pertukaran data, penggunaan data penelitian, pemusnahan data, dan penanganan pengaduan pasien. Selain itu, fasilitas kesehatan perlu melakukan penilaian dampak pelindungan data untuk sistem yang memproses data kesehatan dalam jumlah besar atau menggunakan teknologi berisiko tinggi. Pendekatan tersebut sejalan dengan prinsip WHO yang menekankan perlunya penanggung jawab perlindungan data, mekanisme penanganan pelanggaran, dan pembatasan penggunaan data sesuai tujuan awal (WHO, 2024).

Strategi kedua adalah menerapkan pengamanan teknis dan organisasi secara berlapis. Pengamanan teknis dapat meliputi enkripsi data saat disimpan dan dikirim, autentikasi multifaktor, kontrol akses berbasis peran, pemantauan log, segmentasi jaringan, pencadangan berkala, pembaruan perangkat lunak, pengujian penetrasi, serta sistem pemulihan bencana. Pengamanan organisasi dapat dilakukan melalui pelatihan rutin, audit keamanan, simulasi respons insiden, pemeriksaan vendor, dan penunjukan

pejabat atau petugas yang bertanggung jawab atas perlindungan data. Fasilitas kesehatan juga perlu memiliki rencana respons insiden yang mengatur tahapan identifikasi, pembatasan, pemulihan, dokumentasi, pemberitahuan, dan evaluasi setelah terjadi kebocoran. Kerangka keamanan yang menggabungkan kerahasiaan, integritas, ketersediaan, serta kemudahan penggunaan dapat membantu mencegah pengamanan yang terlalu lemah maupun sistem yang terlalu rumit bagi tenaga kesehatan (Lestari dkk., 2024).

Strategi ketiga adalah meningkatkan transparansi dan kendali pasien atas data pribadinya. Fasilitas kesehatan perlu menyediakan pemberitahuan privasi yang menjelaskan jenis data yang dikumpulkan, tujuan pemrosesan, dasar hukum, jangka waktu penyimpanan, pihak yang menerima data, risiko pemrosesan, dan hak pasien. Pasien juga perlu diberikan prosedur yang mudah untuk mengakses, memperbaiki, atau memperoleh salinan data mengenai dirinya. Untuk penggunaan data di luar pelayanan, seperti penelitian, publikasi, pengembangan algoritma, atau kepentingan komersial, perlu diterapkan mekanisme persetujuan dan pengamanan tambahan (Suraya dkk., 2026). Data yang digunakan untuk penelitian sebaiknya dianonimkan atau dipseudonimkan, sedangkan akses terhadap data identitas harus dibatasi. Dengan meningkatkan transparansi, kepercayaan pasien terhadap pelayanan kesehatan digital dapat dibangun secara lebih berkelanjutan (Sun dkk., 2025).

Strategi keempat adalah memperkuat pengawasan, koordinasi, dan penegakan hukum. Pemerintah perlu menyusun standar keamanan minimum yang dapat diterapkan oleh rumah sakit besar maupun fasilitas kesehatan kecil, disertai dukungan teknis dan pembiayaan yang proporsional. Pengawasan tidak hanya dilakukan setelah kebocoran terjadi, tetapi juga melalui audit kepatuhan, pemeriksaan keamanan, pelaporan berkala, dan evaluasi terhadap penyedia teknologi. Koordinasi antara kementerian, lembaga perlindungan data, pemerintah daerah, organisasi profesi, fasilitas kesehatan, dan penyedia teknologi perlu diperjelas agar tidak terjadi tumpang tindih kewenangan. Penelitian mengenai perlindungan privasi dalam Rekam Medis Elektronik menunjukkan bahwa lemahnya standar keamanan, rendahnya kesadaran tenaga medis, dan pengawasan yang belum optimal merupakan hambatan utama dalam pelaksanaan perlindungan data pasien (Mandey, 2025).

Strategi kelima adalah membangun pendekatan perlindungan data yang berkelanjutan dan berorientasi pada hak pasien. Perlindungan data tidak boleh hanya dilakukan ketika sistem baru dibangun atau setelah terjadi kebocoran, tetapi harus menjadi bagian dari seluruh siklus pengembangan dan penggunaan teknologi kesehatan. Setiap inovasi, termasuk aplikasi kesehatan, telemedicine, kecerdasan buatan, dan integrasi data nasional, perlu dirancang dengan prinsip *privacy by design* dan *security by design*. Artinya, privasi dan keamanan harus dipertimbangkan sejak tahap perencanaan, bukan ditambahkan setelah sistem selesai. Penguatan tersebut perlu disertai evaluasi berkala terhadap efektivitas regulasi, kesiapan infrastruktur, kompetensi sumber daya manusia, dan kepuasan pasien (Siregar & Astuti, 2025). Dengan menggabungkan kepastian

hukum, tata kelola, teknologi, edukasi, serta pengawasan, digitalisasi kesehatan di Indonesia dapat berkembang tanpa mengorbankan kerahasiaan dan hak dasar pasien.

Kesimpulan

Perlindungan hukum data pribadi pasien dalam digitalisasi pelayanan kesehatan di Indonesia memiliki dasar hukum yang cukup kuat melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, dan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. Data kesehatan dikategorikan sebagai data pribadi spesifik yang memerlukan perlindungan lebih tinggi karena berkaitan dengan kondisi fisik, mental, riwayat penyakit, diagnosis, dan informasi medis pasien. Kerangka hukum tersebut memberikan hak kepada pasien untuk memperoleh informasi, mengakses, memperbaiki, dan mengendalikan penggunaan data pribadinya, sekaligus menetapkan kewajiban bagi fasilitas pelayanan kesehatan untuk menjaga kerahasiaan, keamanan, integritas, dan ketersediaan data pasien.

Digitalisasi pelayanan kesehatan melalui Rekam Medis Elektronik, telemedicine, aplikasi kesehatan, dan pertukaran data antar fasilitas kesehatan memberikan manfaat berupa peningkatan efisiensi, kecepatan, dan kesinambungan pelayanan. Namun, penerapannya masih menghadapi sejumlah tantangan, seperti kebocoran data, serangan siber, akses tanpa kewenangan, keterbatasan infrastruktur, rendahnya literasi digital, ketidaksiapan sumber daya manusia, serta penggunaan pihak ketiga dalam pengelolaan sistem. Selain itu, masih diperlukan harmonisasi antara berbagai peraturan agar tidak terjadi ketidakjelasan mengenai tanggung jawab rumah sakit, tenaga kesehatan, penyedia teknologi, dan pihak lain yang memproses data pasien.

Penguatan perlindungan data pasien perlu dilakukan melalui penerapan tata kelola data yang jelas, pembatasan akses berdasarkan kewenangan, enkripsi, autentikasi multifaktor, pencadangan data, audit keamanan, pelatihan tenaga kesehatan, dan mekanisme penanganan insiden yang efektif. Fasilitas pelayanan kesehatan juga harus meningkatkan transparansi kepada pasien mengenai tujuan, dasar hukum, dan pihak yang memproses data pribadi. Dengan menggabungkan kepastian hukum, keamanan teknologi, peningkatan kapasitas sumber daya manusia, pengawasan, dan penghormatan terhadap hak pasien, digitalisasi pelayanan kesehatan di Indonesia dapat berkembang secara aman, bertanggung jawab, dan tetap berorientasi pada perlindungan privasi serta kepentingan pasien.

Daftar Rujukan

Angraeni, W. O. N., Takke, J. A. M., & Kamaruddin, M. I. (2026). Digital Governance and Health Innovation for Strengthening Community Health Systems: A Cross-Sectional Study in Indonesia. *Journal Interdisciplinary Health*, 2(2), 83–91. https://doi.org/10.61099/jih.v2i2.258

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

Lestari, A. Y., Misran, M., Raharjo, T., Annas, M., Riskanita, D., & Prabandari, A. P. (2024). Improving Healthcare Patient Data Security: An Integrated Framework Model For Electronic Health Records From A Legal Perspective. *LAW REFORM*, *20*(2), 329–352. https://doi.org/10.14710/lr.v20i2.56986

Lukitasari, D. A., Zamroni, M., & Putera, A. P. (2023). Hospital Legal Responsibilities for Misuse of Patient Personal Data In Electronic Medical Records. *JILPR Journal Indonesia Law and Policy Review*, *5*(1), 60–74. https://doi.org/10.56371/jirpl.v5i1.164

Mandey, A. W. (2025). Legal Analysis of Patient Privacy Violation in Electronic Medical Records and its Implications for Health Data Protection in Indonesia. *Jurnal Multidisiplin Sahombu*, *5*(02), 589–594.

Nocker, M., & Sena, V. (2019). Big Data and Human Resources Management: The Rise of Talent Analytics. *Social Sciences*, *8*(10), 273. https://doi.org/10.3390/socsci8100273

Nugroho, F. N. P., Listanto, M. F., Amelia, N., & Annisa, S. (2024). Analisis Kebocoran Data Pribadi Dalam Media Sosial. *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen Dan Keuangan*, *1*(2), 58–65. https://doi.org/10.63217/fibonacci.v1i2.70

Putri, T. S., & Putra, M. R. S. (2024). Implementasi Undang-Undang Pelindungan Data Pribadi: Peran Manajemen Risiko Hukum bagi Prosesor Data Pribadi. *Jurnal Hukum Lex Generalis*, *5*(4). https://ojs.rewangrencang.com/index.php/JHLG/article/view/730

Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *8*(1), 70–83. https://doi.org/10.38043/jah.v8i1.6793

Riyantori, R., & Buka, S. P. Y. (2025). Digital Transformation in Primary Health Care: Evaluation of Information Technology Adoption and Management Practices. *Smart International Management Journal*, *2*(4), 48–55. https://doi.org/10.70076/simj.v2i4.129

Safitri Rahmadaniah, A., & Harmanto, D. (2024). *ANALISIS PENYEBAB BELUM TERLAKSANANYA REKAM MEDIS ELEKTRONIK (RME) DI PUSKEMAS PERAWATAN LUBUK TAPI BENGKULU SELATAN* [Other, Sekolah Tinggi Ilmu Kesehatan Sapta Bakti]. https://repository.stikessaptabakti.ac.id/478/

Salijeni, G., Samsonova-Taddei, A., & Turley, S. (2018). *Big Data and Changes in Audit Technology: Contemplating a Research Agenda* (SSRN Scholarly Paper No. 3148904). Social Science Research Network. https://papers.ssrn.com/abstract=3148904

Santo, M. F. O. da, Sari, L., Kamilah, A., & Reumi, F. (2024). *Pengantar Hukum Perdata: Teori & Referensi Komprehensif Dasar-dasar Hukum Perdata di Indonesia*. PT. Sonpedia Publishing Indonesia.

Siregar, R. A., & Astuti, N. K. (2025). Assessing legal and institutional readiness for patient data protection in the age of big health data: An empirical study of health facilities in Indonesia. *International Journal of Law, Policy and Social Review*, *7*(3), 15–21.

Sun, J., Fan, Z., Kou, M., Wang, X., Yue, Z., & Zhang, M. (2025). Impact of nurse-led self-management education on type 2 diabetes: A meta-analysis. *Frontiers in Public Health*, *13*. https://doi.org/10.3389/fpubh.2025.1622988

Suraya, A., Maryuni, Aryanie, D., Lelitasari, Sulandari, U., Setyawati, M., Narulita, S., Jenie, R. P., Ningsih, S. U., Kusrini, E., Triwibowo, A. C., Suyanti, T., Soeharno, R., & Shetye, M. (2026). Childhood Lead Exposure in Primary Health Care Settings in Indonesia: A

Cross-Sectional Study in Bogor City and Bogor Regency. *International Journal of Environmental Research and Public Health*, *23*(8), 1046. https://doi.org/10.3390/ijerph23081046

Susilo, D., Wulandari, L. P. L., Sukmayeti, E., Asante, A., Jan, S., Thabrany, H., Tangcharoensathien, V., Wiseman, V., & Liverani, M. (2025). Can Indonesia achieve universal health coverage? Organisational and financing challenges in implementing the national health insurance system. *SSM - Health Systems*, *5*, 100138. https://doi.org/10.1016/j.ssmhs.2025.100138

Syadina, A., Putra, D. H., Sonia, D., & Satrya, B. A. (2025). TRANSFORMASI RME DI RUMAH SAKIT INDONESIA: TINJAUAN PMK NOMOR 24 TAHUN 2022. *PROSIDING SEMINAR NASIONAL REKAM MEDIS DAN INFORMASI KESEHATAN*, *1*(1). https://prosiding.esaunggul.ac.id/index.php/RMIK/article/view/349

Takaryanto, D., & Lany, A. (2025). Legal Protection of Personal Data in the Exchange of Electronic Medical Record in Healthcare Services. *Research Horizon*, *5*(6), 2817–2830. https://doi.org/10.54518/rh.5.6.2025.897

Udiana, G. K., & Pramana, I. B. N. T. (2025). Legal protection of patients in Indonesia's National Health Insurance (JKN) era: A comprehensive review of regulatory framework and hospital practice. *Dharmaputra Medical Law Journal*, *1*(2), 21–26. https://doi.org/10.51559/rmpp6519

Ventura, M., & Coeli, C. M. (2018). Beyond privacy: The right to health information, personal data protection, and governance. *Cadernos de Saúde Pública*, *34*, e00106818. https://doi.org/https://doi.org/10.1590/0102-311X00106818

Versaci, G. (2018). Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection. *European Review of Contract Law*, *14*(4), 374–392. https://doi.org/10.1515/ercl-2018-1022

Walliman, N., & Walliman, N. (2021). *Research Methods: The Basics* (3 ed.). Routledge. https://doi.org/10.4324/9781003141693

Widyawati, A. M. J., Legowo, M. I., & Purnomo, H. (2025). The Validity of Electronic Agreements in the Perspective of Indonesian Civil Law. *International Journal of Health, Economics, and Social Sciences (IJHESS)*, *7*(2), 749~753-749~753. https://doi.org/10.56338/ijhess.v7i2.7218

Wiley, L. F., & Gostin, L. O. (2025). *Public Health Law and Ethics: Power, Duty, Restraint*. Univ of California Press.

Xiaying, M. (2019). The Legal Attributes of Electronic Data and the Positioning of Data in Civil Law*. *Social Sciences in China*, *40*(1), 82–99. https://doi.org/10.1080/02529203.2018.1519208

Yandi, R., Zuhri, B., Yatim, Y., & Kaksim, K. (2025). The Implementation and Historical Perspective of Health Law in Law No. 17 of 2023. *TOFEDU: The Future of Education Journal*, *4*(6), 2492–2499. https://doi.org/10.61445/tofedu.v4i6.786

Yu, X., & Zhao, Y. (2019). Dualism in data protection: Balancing the right to personal data and the data property right. *Computer Law & Security Review*, *35*(5), 105318. https://doi.org/10.1016/j.clsr.2019.04.001

Zhang, N., Li, Q., Chen, S., Wu, Y., Xin, B., Wan, Q., Shi, P., He, Y., Yang, S., & Jiang, W. (2024). Effectiveness of nurse-led electronic health interventions on illness management in patients with chronic heart failure: A systematic review and meta-analysis. *International Journal of Nursing Studies*, *150*, 104630. https://doi.org/10.1016/j.ijnurstu.2023.104630

Kementerian Kesehatan Republik Indonesia. (2022). *Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis*. Berita Negara Republik Indonesia Tahun 2022 Nomor 829.
Kementerian Kesehatan Republik Indonesia. (2022a). *Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis*. Berita Negara Republik Indonesia Tahun 2022 Nomor 829.
Kementerian Kesehatan Republik Indonesia. (2022a). *Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis*. Berita Negara Republik Indonesia Tahun 2022 Nomor 829.
Kementerian Kesehatan Republik Indonesia. (2022b, September 9). *Fasyankes wajib terapkan rekam medis elektronik*.
Kementerian Kesehatan Republik Indonesia. (2022b, September 9). *Fasilitas pelayanan kesehatan wajib menerapkan rekam medis elektronik*.
Kementerian Komunikasi dan Informatika Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. JDIH Kementerian Komunikasi dan Informatika.
Republik Indonesia. (2022a). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Jakarta: Sekretariat Negara.
Republik Indonesia. (2023). *Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan*. Jakarta: Sekretariat Negara.
Republik Indonesia. (2023). *Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan*. Jakarta: Sekretariat Negara.
Republik Indonesia. (2024). *Peraturan Pemerintah Republik Indonesia Nomor 28 Tahun 2024 tentang Peraturan Pelaksanaan Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan*.
World Health Organization. (2021). *Global strategy on digital health 2020–2025*. Geneva: World Health Organization.
World Health Organization. (2024). *Indonesia digital health transformation strategy 2024*. Geneva: World Health Organization.
World Health Organization. (2024). *WHO personal data protection policy*. Geneva: World Health Organization.
World Health Organization. (2024). *WHO personal data protection policy*. World Health Organization.
World Health Organization. (2025). *Global strategy on digital health 2020–2027*. World Health Organization.