Amnesti: Jurnal Hukum
Vol. 7 No. 2 (2025) pp. 295-305
p-ISSN: 2656-3029 | e-ISSN: 2775 - 0604

Aspek Hukum Perlindungan Data Pasien dalam Implementasi Rekam Medis Elektronik (EMR) di Era Digital

Noor Rahmad[1*], Eren Arif Budiman[2]
[1*]Universitas Muhammadiyah Gombong, Jawa Tengah, Indonesia
[2]Universitas Cenderawasih, Jayapura, Indonesia
*email: noorrahmad@unimugo.ac.id

DOI: https://doi.org/10.37729/amnesti.v7i2.6321

Submitted: Juni 2025 *Revision: Juli 2025* *Accepted: Agustus 2025*

Kata Kunci:
Perlindungan Data Pasien, Rekam Medis Elektronik, Era Digital

ABSTRAK

Dengan kemajuan teknologi, media rekam pun berkembang menjadi Rekam Medis Elektronik (EMR) yang tunduk pada aturan Peraturan Kementerian Kesehatan Nomor 24 Tahun 2022. Namun, kesediaan institusi layanan kesehatan untuk memberikan akses kepada pemerintah terhadap ESDM berisiko melemahkan hak asasi manusia dan privasi, perlindungan data pribadi, dan pengungkapan informasi publik. Terdapat 94 kasus kebocoran data di Republik Indonesia sejak tahun 2019, dan 35 diantaranya terjadi pada tahun 2023. Terkait dengan kewajiban membuka akses ESDM kepada pemerintah, perlu ditinjau kembali perlindungan hukum terhadap kerahasiaan data pasien, Penilaian kepatuhan akses terhadap prinsip perlindungan hukum pasien dan penerapan perlindungan kerahasiaan data RME. Penelitian normatif merupakan metode penelitian deskriptif yang bertujuan untuk menyediakan data yang sistematis dan rinci berdasarkan unsur-unsur yang terkait dengan perlindungan data pribadi. Hasil penelitian menunjukan bahwa banyak peraturan di Indonesia mengenai perlindungan data pribadi yang telah diberlakukan, namun gagal mengatasi tantangan terkait permasalahan yang muncul. Hal ini menciptakan kepastian hukum sebagai salah satu tujuan dari hukum itu sendiri.

ABSTRACT

Keywords:
Patient Data Protection, Electronic Medical Records, The Digital Age

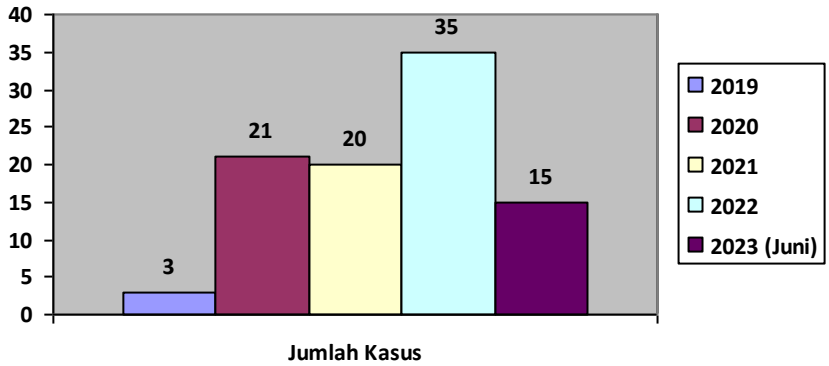
With technological advances, medical records have evolved into Electronic Medical Records (EMR) that are subject to the provisions of Ministry of Health Regulation No. 24 of 2022. However, the willingness of healthcare institutions to grant the government access to EMRs risks undermining human rights and privacy, data protection, and public information disclosure. There have been 94 data breaches in the Republic of Indonesia since 2019, with 35 of them occurring in 2023. Regarding the obligation to grant the government access to EMRs, it is necessary to review legal protections for patient data confidentiality, assess compliance with patient legal protection principles, and implement RME data confidentiality protections. Normative research is a descriptive research method aimed at providing systematic and detailed data based on elements related to personal data protection. The research findings indicate that many regulations in Indonesia regarding personal data protection have been implemented, but they have failed to address the challenges arising from the issues at hand. This creates legal certainty as one of the objectives of the law itself.

1. PENDAHULUAN

Di era digital ini, masyarakat khawatir bahwa teknologi digital dapat mempercepat globalisasi dan membuat dunia semakin terhubung. Namun, hubungan ini juga dapat menimbulkan konsekuensi yang merugikan, seperti munculnya ketegangan digital antara negara maju dan berkembang, dan berisiko memperparah disparitas dalam distribusi kekayaan dan sumber daya. (Meher et al., 2023). Kekhawatiran tersebut dilatarbelakangi oleh kenyataan bahwa teknologi digital di era industri ini tidak hanya menawarkan banyak kemajuan di berbagai bidang kehidupan, seperti komunikasi, transportasi, kesehatan, dan pendidikan, namun juga menawarkan tantangan baru dalam pembangunan masyarakat global yang inklusif, dimana setiap individu mempunyai peluang yang sama untuk berkembang dalam konteks globalisasi yang semakin pesat.

Digitalisasi mengacu pada penggunaan teknologi informasi dan komunikasi untuk meningkatkan efisiensi, aksesibilitas, dan kualitas layanan. (Syahwali et al., 2023). Menganalisis penelitian yang ada, penelitian ini akan mengkaji bukti mengenai pencapaian transformasi digital, termasuk penggunaan sistem informasi medis, rekam medis elektronik, dan aplikasi teknologi kesehatan. Menurut *World Healthy Organization* (WHO), digitalisasi layanan kesehatan telah menjadi tren global dan mewakili cara untuk memastikan layanan kesehatan yang inklusif dan berkualitas (Ikawati & Ansyori, 2023).

Dalam beberapa tahun terakhir, sektor kesehatan menjadi salah satu yang paling terdampak oleh transisi digital. Di era internet dan media sosial, pelanggaran keamanan yang melibatkan data pribadi pasien di rumah sakit dapat dengan cepat tersebar luas. Setelah insiden semacam ini, kepercayaan masyarakat terhadap kemampuan rumah sakit melindungi informasi pribadi akan menurun (Yunus et al., 2019). Akibatnya, sebagian orang enggan mencari pertolongan medis karena khawatir rekam medis mereka terbuka untuk publik, dan memilih mencari alternatif lain (Tampubolon et al., 2024). Diketahui sejak 2019 hingga 2024, tercatat 94 kasus kebocoran data di Indonesia, sebagian besar di antaranya 62 kasus melibatkan Penyelenggara Sistem Elektronik (PSE) privat atau swasta (Anisah, 2023). Seluruh PSE yang terlibat telah menerima teguran dan rekomendasi perbaikan. Berikut **Gambar 1.** Jumlah Kasus Kebocoran data di Indonesia periode 2019 – 2023.



Gambar 1. *Jumlah Kasus Kebocoran Data di Indonesia Tahun 2019 - 2023*

Perkembangan teknologi digital telah menciptakan perspektif baru dalam layanan kesehatan, secara signifikan mengubah cara rumah sakit dan penyedia layanan kesehatan berinteraksi dengan pasien, mengelola informasi perangkat medis, serta meningkatkan efisiensi prosedur perawatan. Digitalisasi, melalui pemanfaatan beragam alat dan teknologi, menjadi langkah penting dalam evolusi layanan kesehatan rumah sakit.

Seluruh rumah sakit milik Pemerintah Provinsi Jawa Tengah telah mengimplementasikan sistem layanan berbasis elektronik, meskipun dengan sejarah dan metode pengembangan yang beragam. Perbedaan terlihat pada media, aplikasi, dan bahasa pemrograman yang digunakan. Secara umum, layanan ini mencakup proses pendaftaran pasien, informasi jadwal layanan, dan administrasi. Beberapa rumah sakit telah mengembangkan layanan dalam

bentuk situs web, sebagian lainnya dilengkapi aplikasi Android, serta menerapkan sistem pendaftaran elektronik sebagai metode utama (Nadiroh & Wiraguna, 2025).

Keamanan rekam medis menjadi perhatian serius mengingat jumlah dan sumber data yang diungkapkan, sebagaimana dilaporkan Kementerian Kesehatan. Koalisi Advokasi Hak Individu atas Privasi turut menyoroti persoalan ini, dan menurut Direktur Eksekutif ELSAM, Kementerian Kesehatan menangani informasi pribadi pasien Covid-19 sebagai bagian dari sistem informasi kesehatan elektronik. Teknologi informasi kesehatan mencakup seluruh sistem komputer yang digunakan untuk menyimpan, mengakses, memproses, membagikan, dan mengirimkan informasi kesehatan, sekaligus mendukung penyampaian layanan serta pengelolaan sistem kesehatan. Data yang dikelola bersifat sangat rahasia, meliputi pemeriksaan pasien, diagnosis, pengobatan, dan riwayat kesehatan (Sutabri et al., 2023), sehingga wajib dilindungi dari segala bentuk manipulasi demi menjaga kepercayaan pasien untuk terus berbagi informasi kesehatan dan pekerjaan mereka, dengan tetap memperhatikan tanggung jawab moral maupun hukum. Namun, dinamika dan perubahan cepat dalam lingkungan teknologi informasi kesehatan justru menghadirkan tantangan yang semakin besar terhadap keamanan rekam medis.

Terlepas dari berbagai upaya perlindungan, potensi gangguan terhadap privasi pasien masih kerap terjadi dan bahkan dapat diatasi oleh sistem komersial yang telah ada saat ini. Sentralisasi rekam medis dalam sistem kesehatan, disertai meningkatnya praktik multi-kelompok, membuat data medis pribadi terdistribusi melalui jaringan yang semakin luas. Kondisi ini meningkatkan kemungkinan terjadinya akses atau konsultasi oleh pihak yang tidak berwenang. Semakin banyak pengguna yang terhubung dalam satu sistem, semakin besar pula peluang terjadinya pelanggaran privasi pasien. Berbagai titik rentan dalam sistem rekam medis elektronik (*Electronic Medical Records*/EMR) modern—seperti penggunaan cloud computing, mekanisme distribusi data, dan akses internal—dapat menjadi celah terjadinya kebocoran informasi. Hal ini menguatkan pandangan bahwa distribusi data dalam jaringan berskala besar berbanding lurus dengan tingginya risiko akses tidak sah. Meskipun sistem yang lebih besar umumnya memiliki mekanisme pemantauan terhadap akses ilegal, fasilitas atau kantor satelit yang lebih kecil sering kali tidak memiliki kemampuan serupa untuk mengawasi siapa saja yang mengakses rekam medis pasien (Nurlaila et al., 2024).

Transformasi digital diharapkan mampu memberikan layanan yang lebih efisien, transparan, dan mudah diakses pada seluruh tingkatan penyelenggara layanan, termasuk di sektor kesehatan. Namun, mewujudkan transformasi digital yang inklusif dan berkelanjutan bukanlah hal yang mudah. Sebagai negara kepulauan dengan keragaman geografis dan demografis yang tinggi, Indonesia menghadapi tantangan kompleks dalam mengimplementasikan visi tersebut (Yunita et al., 2023). Salah satu hambatan utama adalah kesenjangan akses digital antar wilayah, yang tidak hanya terjadi antara daerah perkotaan dan perdesaan, tetapi juga antar wilayah di Indonesia. Ketimpangan ini berdampak langsung pada kemampuan sebagian masyarakat untuk mengakses layanan berbasis daring. Faktor geografis, ekonomi, dan sosial menjadi penyebab kesenjangan ini, sehingga menghambat proses integrasi teknologi dalam layanan publik, termasuk layanan kesehatan.

Selain aksesibilitas, peningkatan keterampilan digital masyarakat menjadi kunci agar semua warga negara dapat memanfaatkan layanan publik digital secara efektif. Transformasi digital juga memerlukan perhatian pada aspek krusial seperti perlindungan data dan privasi, perubahan budaya organisasi di lingkungan pemerintahan, koordinasi antarlembaga, dan integrasi sistem. Pemerintah daerah perlu mengadopsi pendekatan yang komprehensif dan kolaboratif dengan visi serta strategi yang terpadu, guna mengatasi tantangan dan memaksimalkan pemanfaatan teknologi demi mewujudkan tata kelola yang transparan, efektif, dan inklusif. Di sisi lain, pengelolaan data kesehatan pribadi di Indonesia masih menghadapi persoalan serius, seperti kebocoran data, penggunaan tanpa izin, dan pembagian lintas negara yang tidak terkendali. Kondisi ini menegaskan bahwa tantangan hukum dan kebijakan terkait pengaturan pemanfaatan data kesehatan pribadi harus menjadi prioritas utama bagi Indonesia.

2. METODE PENELITIAN

Menurut (Sunggono, 2006), penelitian normatif merupakan analisis deskriptif yang bertujuan menyediakan data secara sistematis dan terperinci berdasarkan unsur-unsur yang berkaitan dengan perlindungan data pribadi. Pemilihan bahan pustaka mencakup data dasar suatu bidang ilmu yang tergolong sebagai data sekunder, yaitu data yang diperoleh penulis dari sumber-sumber yang telah ada, seperti dokumen resmi, buku, hasil penelitian berupa laporan, jurnal, dan lainnya (Soekanto & Mamuji, 2011). Dalam

penelitian hukum, data tersebut dilengkapi dengan bahan hukum primer yang bersifat mengikat, antara lain Undang-Undang Dasar Negara Republik Indonesia Tahun 1945; Rancangan Undang-Undang Perlindungan Data Pribadi; Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan; Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik; serta Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

3. HASIL DAN PEMBAHASAN

Di Indonesia, informasi pribadi termasuk data kesehatan masih tergolong rentan mengalami kebocoran dan belum sepenuhnya terlindungi. Kerentanan ini disebabkan oleh ketiadaan regulasi khusus yang secara komprehensif mengatur perlindungan data pribadi, sehingga penyalahgunaan informasi individu kerap terjadi di berbagai platform. Direktur Jenderal Aplikasi dan Informatika Kementerian Komunikasi dan Informatika, Semuel Abrijani Pangerapan, mencatat bahwa sejak 2019 telah terjadi 94 kasus kebocoran data di Indonesia, di mana 62 di antaranya melibatkan PSE privat atau swasta (Anisah, 2023). Seluruh pihak yang mengalami insiden tersebut telah menerima teguran serta rekomendasi perbaikan dari pemerintah.

Kerangka hukum perlindungan data pribadi di Indonesia hingga kini masih bersifat umum dan tersebar dalam berbagai peraturan perundang-undangan, sehingga belum mampu menjawab secara tuntas seluruh persoalan yang berkembang di masyarakat. Idealnya, Indonesia memerlukan regulasi yang bersifat spesifik, komprehensif, dan responsif terhadap perkembangan teknologi, guna memperkuat keamanan data setiap individu serta memberikan sanksi tegas bagi pelanggar. Hal ini menjadi krusial mengingat data pribadi merupakan aset bernilai yang mencerminkan identitas seseorang dan dapat dimanfaatkan untuk tujuan yang sah maupun yang berpotensi merugikan.

Perlindungan data pribadi merupakan kewajiban konstitusional, sejalan dengan Pasal 1 ayat (3) Undang-Undang Dasar 1945 (UUD 1945) yang menegaskan bahwa Indonesia adalah negara hukum. Sebagai negara hukum sekaligus negara demokrasi, Negara Kesatuan Republik Indonesia berkewajiban memberikan jaminan perlindungan hukum bagi setiap warga negara, termasuk dalam menjaga kerahasiaan informasi pribadi. Data pribadi mencakup segala informasi yang dapat mengidentifikasi seseorang, yang

apabila diakses atau digunakan secara tidak sah dapat menimbulkan kerugian material maupun immaterial.

Dalam sektor kesehatan, kebocoran data pribadi memiliki konsekuensi yang sangat serius, terlebih jika menyangkut catatan medis yang bersifat rahasia. Data kesehatan mencakup identitas pasien, hasil laboratorium, diagnosis, tindakan medis, serta riwayat pengobatan baik untuk pasien rawat inap, rawat jalan, maupun layanan darurat. Berdasarkan Peraturan Menteri Kesehatan Nomor 269 Tahun 2008 tentang Rekam Medis, rumah sakit sebagai pengelola sistem elektronik berkewajiban menjaga kerahasiaan identitas dan riwayat kesehatan pasien, kewajiban yang melekat pada administrator, manajer, maupun pimpinan fasilitas pelayanan kesehatan.

Penerapan rekam medis elektronik (*Electronic Medical Record*/EMR) memang membawa manfaat besar dalam hal efisiensi, tetapi juga memunculkan tantangan keamanan. Risiko yang dihadapi meliputi serangan malware atau ransomware, akses tidak sah, kerentanan pada perangkat seluler, hingga ketidakpatuhan terhadap standar keamanan. Untuk mengantisipasinya, diperlukan strategi perlindungan seperti enkripsi data, sertifikasi keamanan, pelatihan keamanan bagi pengguna, serta pemantauan dan deteksi dini ancaman. Langkah-langkah ini penting untuk menjaga integritas, kerahasiaan, dan ketersediaan data medis di tengah perkembangan teknologi kesehatan digital.

Hukum positif Indonesia yang mengatur perlindungan data pribadi masih sangat lemah, hanya memuat ketentuan umum yang tidak menjawab kompleksitas persoalan masa kini. Hingga saat ini belum ada undang-undang yang secara eksplisit mengatur perlindungan data pribadi dari kebocoran. Ketentuan yang ada tersebar di lebih dari 30 peraturan, yang masing-masing hanya membahas sebagian aspek perlindungan tersebut. Kekosongan dan ketidaksinkronan regulasi ini membuat penyalahgunaan data pribadi menjadi lebih mudah terjadi.

Kekurangan kerangka hukum ini telah memunculkan berbagai masalah, salah satunya penggunaan data pribadi secara berlebihan tanpa izin, terutama oleh pihak ketiga. Desakan masyarakat akan hadirnya regulasi khusus mendorong pemerintah menyusun Rancangan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (RUU PDP) sejak 2016. RUU ini memuat pengaturan yang lebih luas dibandingkan peraturan sebelumnya, termasuk membedakan kategori data pribadi umum dan data pribadi khusus, sebagaimana diatur dalam Pasal

Data pribadi umum mencakup nama, jenis kelamin, alamat, dan informasi lain yang dapat diakses secara luas. Jika data ini diungkap tanpa persetujuan, pemilik data dapat mengalami kerugian. Sementara itu, data pribadi khusus menyangkut informasi yang memengaruhi keamanan dan kesejahteraan individu, yang hanya boleh diakses dengan persetujuan pemilik atau berdasarkan ketentuan undang-undang. Dalam konteks layanan kesehatan, tantangan keamanan mencakup penyimpanan data, kesesuaian praktik medis dengan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), dan keberadaan aturan keamanan data telemedicine.

Masalah penyimpanan data kesehatan sangat kompleks. Studi (Annan, 2024) mengungkapkan bahwa pada 2021, sekitar 720 GB data pasien dari berbagai rumah sakit di Indonesia dipublikasikan secara ilegal, mencakup laporan radiologi, hasil laboratorium, hingga surat rujukan BPJS Kesehatan. Infrastruktur penyimpanan memerlukan biaya tinggi untuk server, keamanan, dan pemeliharaan, yang dapat berdampak pada harga layanan dan akses pasien. Sentralisasi data pun memunculkan risiko privasi jika tidak disertai langkah perlindungan yang memadai.

Penyelarasan etika medis dengan UU PDP menjadi keharusan, mencakup prinsip kerahasiaan, keterbukaan, dan otonomi pasien. Penelitian (Sulaiman et al., 2022) menegaskan bahwa rumah sakit yang memanfaatkan telemedicine wajib menjamin privasi data pasien, termasuk dengan memperoleh sertifikasi keamanan sistem. UU PDP mengharuskan penyedia layanan memberi informasi jelas kepada pasien mengenai pengumpulan, penggunaan, dan pembagian data pribadi, serta memperoleh persetujuan yang diinformasikan sebelum memproses data tersebut.

Akses dan pengelolaan informasi pasien harus dibatasi hanya kepada pihak berwenang. Penyedia telemedicine wajib mematuhi peraturan, memberitahu pasien jika terjadi pelanggaran, serta menghormati hak pasien untuk mengakses dan menghapus data pribadi mereka. Pelatihan etika dan kepatuhan bagi tenaga medis menjadi langkah strategis untuk meningkatkan kesadaran akan pentingnya kerahasiaan data.

Dalam lingkup hukum, telemedicine diatur dalam Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan serta Permenkes Nomor 20 Tahun 2019 tentang Penyelenggaraan Pelayanan Telemedicine Antar Fasilitas Pelayanan Kesehatan. Namun, penelitian (Mustikasari, 2021) menunjukkan bahwa aturan ini masih terbatas pada telemedis antar-institusi kesehatan dan belum mengatur secara rinci aspek keamanan data pasien. Banyak platform

konsultasi online belum memenuhi persyaratan sebagai penyelenggara telemedis resmi sesuai ketentuan pemerintah.

Perlindungan keamanan data dalam telemedicine membutuhkan langkah teknis seperti enkripsi komunikasi antara pasien dan penyedia layanan, mekanisme autentikasi ganda, serta pengawasan sistem untuk mendeteksi potensi pelanggaran. Praktik internasional seperti *Health Insurance Portability and Accountability Act* (HIPAA), sebuah undang-undang federal Amerika Serikat yang ditetapkan pada tahun 1996. Tujuan utamanya adalah untuk memberikan perlindungan dan privasi data kesehatan individu. HIPAA berlaku untuk entitas yang menangani informasi kesehatan yang dilindungi (PHI), seperti rumah sakit, penyedia layanan kesehatan, perusahaan asuransi, dan lainnya yang dapat menjadi acuan dalam menetapkan standar privasi data medis. Selain itu, edukasi berkelanjutan bagi pasien, tenaga medis, dan penyedia layanan sangat penting untuk mengurangi risiko kebocoran data.

Rumah sakit sebagai pengendali data wajib memperoleh persetujuan pasien sebelum memproses data kesehatan, kecuali dalam keadaan darurat yang mengancam nyawa. Pasien juga memiliki hak untuk menarik persetujuan, membatasi pemrosesan data, dan memperoleh informasi tentang setiap perubahan data kesehatan mereka. Rumah sakit bertanggung jawab menjaga keamanan data, mencegah penyalahgunaan, serta mencatat setiap aktivitas pemrosesan.

RUU PDP membawa perubahan signifikan dengan mengatur praktik-praktik yang sebelumnya belum tersentuh, seperti pelarangan penjualan data pribadi. Negara-negara seperti Singapura, Malaysia, Amerika Serikat, dan berbagai negara Eropa telah memiliki undang-undang khusus yang memberikan perlindungan kuat bagi data pribadi. Indonesia perlu segera mengadopsi regulasi serupa untuk memastikan keamanan data pribadi, khususnya data kesehatan, sehingga masyarakat dapat memperoleh layanan medis digital yang aman, andal, dan sesuai dengan prinsip negara hukum.

4. KESIMPULAN

Berdasarkan uraian di atas dapat disimpulkan bahwa perlindungan data pribadi, khususnya data kesehatan, merupakan kewajiban fundamental negara hukum yang bersumber dari Pasal 1 ayat (3) UUD 1945 dan sejalan dengan Pasal 28G ayat (1) UUD 1945 yang menjamin hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda. Dalam konteks kesehatan, kewajiban ini dipertegas melalui Pasal 57 ayat (1)

Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan yang mewajibkan setiap tenaga kesehatan merahasiakan segala sesuatu yang diketahui tentang pasien, serta Permenkes Nomor 269 Tahun 2008 tentang Rekam Medis yang mengatur kewajiban fasilitas pelayanan kesehatan untuk menjaga kerahasiaan informasi pasien. Namun, kenyataannya regulasi yang ada masih bersifat sektoral dan parsial, sehingga belum mampu menjawab tantangan keamanan data di era digital. Kehadiran Rancangan Undang-Undang Perlindungan Data Pribadi menjadi krusial untuk membentuk kerangka hukum yang komprehensif, termasuk mengatur klasifikasi data pribadi umum dan khusus, kewajiban persetujuan pemilik data, mekanisme keamanan, serta sanksi bagi pelanggar. Mengacu pula pada Pasal 26 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya dalam UU Nomor 19 Tahun 2016, yang menegaskan bahwa penggunaan data pribadi harus dilakukan dengan persetujuan pemilik data, jelas bahwa sinergi lintas peraturan diperlukan agar perlindungan data pribadi dapat terlaksana secara efektif. Dengan demikian, urgensi pembentukan undang-undang khusus perlindungan data pribadi, yang harmonis dengan prinsip kerahasiaan medis dan perkembangan teknologi kesehatan digital, menjadi keharusan demi menjamin hak konstitusional warga negara serta mencegah kerugian material maupun immaterial akibat kebocoran informasi sensitif.

DAFTAR PUSTAKA

Anisah, L. (2023). *Kominfo: Sejak 2019 hingga Juni 2023 Tercatat Ada 94 Kasus Kebocoran Data Pribadi*. News Setup. https://newssetup.kontan.co.id/news/kominfo-sejak-2019-hingga-juni-2023-tercatat-ada-94-kasus-kebocoran-data-pribadi

Annan, A. (2024). Tinjauan Yuridis Perlindungan Data Pribadi Pada SektorKesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022. *SYNERGY Jurnal Ilmiah Multidisiplin*, *1*(4), 247–254.

Ikawati, F. R., & Ansyori, A. (2023). Tantangan Rekam Medis Elektronik Dalam Perlindungan Data Pribadi Challenges of Electronic Medical Records in. *Prosiding Seminar Nasional Rekam Medis & Manajemen Informasi Kesehatan*, 10–18.

Meher, C., Sidi, R., & Risdawati, I. (2023). Penggunaan Data Kesehatan Pribadi Dalam Era Big Data: Tantangan Hukum dan Kebijakan di Indonesia. *Jurnal Ners*, *7*(2), 864–870. https://doi.org/10.31004/jn.v7i2.16088

Mustikasari, A. P. (2021). Informed Consent dan Rekam Medis dalam

Telemedicine di Indonesia. *Jurnal Hukum Dan Pembangunan Ekonomi*, *8*(2), 89. https://doi.org/10.20961/hpe.v8i2.49759

Nadiroh, A., & Wiraguna, S. A. (2025). Analisis Yuridis Kebocoran Data di Layanan Kesehatan Digital: Studi Kasus Aplikasi Telemedicine di Indonesia. *Media Hukum Indonesia (MHI)*, *2*(6), 313–320.

Nurlaila, Zuriatin, & Nurhasanah. (2024). Transformasi Digital Pelayanan Publik: Tantangan dan Prospek dalam Implementasi E-Government di Kabupaten Bima. *Public Service and Governance Journal*, *5*(2), 21–37. https://doi.org/10.56444/psgj.v5i2.1468

Soekanto, S., & Mamuji, S. (2011). *Penelitian Hukum Normatif Suatu Tinjauan Singkat*.

Sulaiman, E., Handayani, T., & Mulyana, A. (2022). Juridical Study of Telemedicine Consulting Services in Indonesia. *Soepra: Jurnal Hukum Kesehatan*, *7*(2), 259–274. https://doi.org/10.24167/shk.v7i2.3545

Sunggono, B. (2006). *Metodologi Penelitian Hukum*. PT Raja Grafindo Persada.

Sutabri, T., Enjelika, D., Mujiranda, S., & Virna, L. (2023). Transformasi Digital di Puskesmas Menuju Pelayanan Kesehatan yang Lebih Efisien dan Berkualitas. *IJM: Indonesian Journal of Multidisciplinary*, *1*(5), 1705–1716.

Syahwali, A. J., Piwari, B., Prabowo, A., & Sutabri, T. (2023). Transformasi Digital untuk Pengembangan Pelayanan Kesehatan di Rumah Sakit. *IJM: Indonesian Journal of Multidisciplinary*, *1*(5), 1770–1777.

Tampubolon, E. T. F., Putera, A. P., & Huda, M. K. (2024). Pertanggungjawaban Hukum Rumah Sakit Terkait Kebocoran Data Pribadi Pasien Berdasarkan Peraturan Perundang-Undangan. *Syntax Idea*, *6*(3).

Yunita, A. R., Sari, S. P., Putri, F. E., Felissia, D. S., Fadhillana, Y. R., & Arizzal, N. Z. (2023). Hukum Perdata Nasional di Era Digital: Tantangan dan Peluang Dalam Perlindungan Data Pribadi. *Proceeding of Conference on Law and Social Studies*, *4*(1), 1–11.

Yunus, M., Kesuma, T. M., Diah, M., Yusuf, F., Abubakar, A., Rizal, S., Putra, C., Musnadi, S., Siregar, M. R., Oktaviza, Y., & Zikran, G. (2019). *Hospitality Hospital Management*. Syiah Kuala University Press.