BACARITA Law Journal
Volume 6 Issue 2, April 2026: p. 290 - 304
E-ISSN: 2775-9407
: 10.30598/bacarita.v6i2.23679

Personal Data Protection for Health Data Security Governance in E-Health System

Perlindungan Data Pribadi Terhadap Tata Kelola Keamanan Data Kesehatan Pada Sistem E-Health

Nazwa Putri Mbuinga[1*], Inayah R Bempah[2], Zalwa Natasha Anggreini Manoppo[3]

[1,2,3] Faculty of Law, Universitas Negeri Gorontalo, Gorontalo, Indonesia.
: nazwaputriiii11@gmail.com
Corresponding Author*

Abstract

Personal data, including medical information, is highly vulnerable to leaks, which can trigger various cybercrimes such as identity theft and fraud. This study uses a normative legal approach with conceptualization methods and a review of legislation to examine the challenges and solutions in implementing data protection in accordance with Law Number 27 of 2022. The research findings indicate that despite increasingly strengthened legal support, various obstacles such as low public awareness, limited law enforcement resources, and complexity remain major barriers. Therefore, it is recommended that regulations be harmonized, encryption technology implemented, and public literacy and training for healthcare providers be improved to maintain patient data privacy and security.

Keywords: Personal Data Protection; E-Health; Data Security Governance.

Abstrak

Data pribadi, termasuk informasi medis, memiliki tingkat kerentanan yang tinggi terhadap kebocoran, yang dapat memicu berbagai tindak kejahatan siber seperti pencurian identitas dan penipuan. Penelitian ini menggunakan pendekatan hukum normatif dengan metode konseptualisasi serta kajian peraturan-undangan untuk menelaah tantangan dan solusi dalam pelaksanaan perlindungan data sesuai dengan ketentuan Undang-Undang Nomor 27 Tahun 2022. Temuan penelitian menunjukkan bahwa meskipun dukungan hukum semakin diperkuat, berbagai kendala seperti rendahnya kesadaran masyarakat, keterbatasan sumber daya aparat penegak hukum, serta kompleksitas masih menjadi hambatan utama. Oleh karena itu, direkomendasikan perlunya harmonisasi regulasi, penerapan teknologi enkripsi, serta peningkatan literasi publik dan pelatihan bagi penyedia layanan kesehatan sebagai upaya menjaga privasi dan keamanan data pasien.

Kata Kunci: Perlindungan Data Pribadi; E-Health; Tata Kelola Keamanan Data.

Submitted: 2025-12-10 *Revised: 2026-03-07* *Accepted: 2026-03-27* *Published: 2026-04-30*

How To Cite: Nazwa Putri Mbuinga, Inayah R Bempah, and Zalwa Natasha Anggreini Manoppo. "Personal Data Protection for Health Data Security Governance in E-Health System." *BACARITA Law Journal* 6 no. 2 (2026): 290-304. https://doi.org/10.30598/bacarita.v6i2.23679

Copyright © 2026 Author(s) Creative Commons Attribution-NonCommercial 4.0 Internasional License

PENDAHULUAN

Data pribadi meliputi berbagai informasi penting, seperti identitas, alamat, nomor telepon, tanggal lahir, riwayat kesehatan, serta aktivitas di dunia maya. Data pribadi dalam konteks pendidikan, data siswa, tenaga pendidik, dan orang tua sangat rentan menjadi fokus jika tidak dikelola dan dilindungi secara optimal. Kesadaran serta edukasi mengenai keamanan data menjadi hal yang sangat penting dalam menjaga privasi dan privasi. Sebagian besar kasus besar kebocoran data bukan disebabkan oleh kegagalan teknologi, melainkan akibat kelalaian manusia, seperti penggunaan kata sandi yang tidak kuat,

penyebaran informasi sensitif tanpa kontrol, dan pengabaian terhadap protokol keamanan dasar. Terdapat bukti bahwa data BPJS Ketenagakerjaan yang mencakup informasi dari 279 juta penduduk Indonesia, termasuk data kesehatan, pernah bocor dan diperjualbelikan di forum bold. Kebocoran data pribadi dalam sistem e-Health Indonesia telah menimbulkan berbagai tindak kejahatan siber, mulai dari pencurian identitas, pemerasan, hingga penipuan klaim asuransi kesehatan. Perlindungan terhadap data pribadi merupakan bagian dari hak asasi manusia yang diatur secara tegas dalam Pasal 28G Undang-Undang Dasar 1945. Digitalisasi di sektor kesehatan mengalami perkembangan signifikan dalam beberapa tahun terakhir melalui penerapan e-Health, seperti penggunaan aplikasi kesehatan, layanan telemedicine, serta sistem rekam medis elektronik (RME).[1]

E -Healt adalah bagian dari rencana aksi Aksi *World Summit on the Information Society* (WSIS) Jenewa 2003, adalah aplikasi yang berbasis teknologi informasi dan komunikasi (TIK) yang digunakan dalam industri layanan kesehatan. Penerapan E-Healt bertujuan untuk meningkatkan akses, efisiensi, efiktifitas, serta kualitas proses medis yang melibatkan berbagai organisasi pelayanan kesehatan seperti rumah sakit, klinik, puskesmas, praktisi medis baik dokter maupun terapis, laboratorium, apotek, dan perusahaan asuransi, sekaligus pasien sebagai konsumen. Namun, dalam pelaksanaan layanan melalui *e-health*, dikumpulkan data pribadi konsumen yang bersifat sensitif, sehingga menimbulkan persoalan hukum baru terkait sejauh mana penyedia layanan kesehatan mampu melindungi data pribadi pasien agar tidak mudah di akses maupun disebarluaskan akibat kemajuan TIK.[2]

Indonesia adalah negara berkembang yang menghadapi berbagai masalah dan tantangan dalam bidang kesehatan masyarakat. Pengembangan serta pemanfaatan telemedicine dan *e-health* dan bidang terkait lainnya memberikan banyak peluang untuk membantu mengatasi permasalahan dan tantangan tersebut. Berbagai aplikasi yang dapat digunakan meliputi pencatatan dan pelaporan, manajemen wabah, resep elektronik, manajemen pasien tuberkulosis, sistem telemedicine seluler, e-psikologi, e-kesehatan seluler, berbagai jenis sistem e-health dengan pengiriman gambar, serta sistem open-EHR (*Electronic health record*)yang bersifat terbuka.[3] Perlindungan data kesehatan, tidak hanya dipahami semata-mata sebagai persoalan teknis, akan tetapi juga sebagai bagian dari hak asasi manusia, khususnya hak atas privasi, martabat, serta perlindungan dari penyalahgunaan informasi yang berpotensi merugikan individu. Perspektif ini menekankan bahwa perlindungan data merupakan sarana untuk menjaga kebebasan dan kesetaraan dalam memperoleh perlindungan data, dengan memastikan setiap orang terutamanya kelompok yang rentan tidak mengalami kerugian akibat penggunaan data kesehatan yang tidak adil atau eksploitatif. Maka dari itu perlindungan terhadap data pribadi merupakan sesuatu yang perlu diperhatikan dan dilindungi secara serius.[4]

Perkembangan teknologi informasi di era digital telah menciptakan tren, budaya, serta pola perilaku baru dalam masyarakat, yang dapat bersifat positif, negatif, maupun

---

[1] Indah Susilowati, Lia Agustina, and Ratna Frenty Nurkhalim. "Edukasi Mengenai Upaya Menjaga Privasi Data Pribadi Dalam Penggunaan E-Health." *Journal of Community Engagement and Empowerment* 7, no. 1 (2025): 63-69. https://www.ojs.iik.ac.id/index.php/JCEE/article/view/963

[2] Handryas Prasetyo Utomo, Elisatris Gultom, and Anita Afriana. "Urgensi Perlindungan Hukum Data Pribadi Pasien dalam Pelayanan Kesehatan Berbasis Teknologi di Indonesia." *Jurnal Ilmiah Galuh Justisi* 8, no. 2 (2020): 168-185.

[3] Sinta Dewi Rosadi. "Implikasi Penerapan Program E-Health Dihubungkan Dengan Perlindungan Data Pribadi. Arena Hukum" 9, no. 3 (2016): 403-420. https://doi.org/10.21776/ub.arenahukum.2016.00903.6

[4] Alaikha Annan. "Tinjauan Yuridis Perlindungan Data Pribadi Pada Sektor Kesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022". *Sinergi: Jurnal Ilmiah Multidisiplin* 1, no. 4 (2023): 247–254.

BACARITA Law Journal, 6 (2) April 2026: 290 - 304
E-ISSN: 2775-9407
Published by: Program Study of Law Outside the Main Campus, Universitas Pattimura, Dobo, Indonesia.

konstruktif. Menghadapi hal ini, pengguna teknologi perlu menerapkan sikap kehati-hatian. Banyak pengguna media sosial, baik secara sadar maupun tidak, seringkali membagikan informasi atau data pribadi mereka melalui platform tersebut, yang pada gilirannya berpotensi meningkatkan risiko kerugian, baik secara finansial maupun non-finansial. Secara umum, kesadaran masyarakat terhadap dampak penyalahgunaan informasi masih relatif rendah, sehingga perlindungan terhadap data pribadi belum mendapat perhatian optimal. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi di Indonesia hadir dengan tujuan utama untuk melindungi data pribadi setiap individu sekaligus mengatur mekanisme pengumpulan, penggunaan, penyimpanan, pengamanan, dan penghapusan data pribadi oleh pihak-pihak yang bertanggung jawab mengelolanya. Adapun beberapa aturan lainnya Peraturan Menteri Kesehatan (Permenkes) Nomor 24 Tahun 2022 tentang Rekam Medis peraturan ini mewajibkan seluruh fasilitas kesehatan menggunakan rekam medis elektronik serta memastikan keamanan data medis pasien, Permenkes Nomor 18 Tahun 2022 tentang Penyelenggaraan Satu Data Bidang Kesehatan, Permenkominfo Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik (PSE) lingkup privat tetapi sudah mengalami perubahan. Peraturan ini telah diubah oleh Permenkominfo Nomor 10 Tahun 2021 menetapkan bahwa kewajiban pendaftaran bagi PSE lingkup privat dilakukan paling lambat 6 bulan sejak penerapan sistem perizinan berusaha berbasis risiko melalui sistem OSS efektif.

Sebuah penelitian di Jakarta berjudul *Perception and Practices of Health Data Privacy Protection among Consumers: An Empirical Study in One of Indonesia's Major Cities* menunjukkan bahwa meskipun konsumen menyadari pentingnya privasi data kesehatan, praktik perlindungan oleh penyelenggara layanan masih memerlukan perbaikan.[5] Selain itu, studi lain mengidentifikasi kendala yang dihadapi fasilitas kesehatan di Indonesia, seperti keterbatasan infrastruktur keamanan, sumber daya manusia, dan budaya organisasi, yang secara signifikan menghambat upaya perlindungan data pasien dalam sistem elektronik (lihat Improving Healthcare Patient Data Security).[6]

Judul	Perbedaan	Persamaan
Perception and Practices of Health Data Privacy Protection among Consumers: An Empirical Study in One of Indonesia's Major Cities	Dari kedua jurnal ini sama-sama membahas tentang perlindungan data kesehatan dan privasi dalam sistem digital	Dalam penelitian ini yang berbasis empiris pada masyarakat, sedangkan dalam jurnal yang kami teliti berbasis hukum normatif dan kebijakan nasional
Tinjauan Yuridis Perlindungan Data Pribadi Pada Sektor Kesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022	Dalam jurnal ini lebih berfokus pada kajian hukum normatif UU PDP sedangkan dalam penelitian yang dilakukan fokus pada	Dari kedua jurnal ini memiliki persamaan dalam mengkaji perlindungan hukum atas data kesehatan

[5] Joni Yusufa, Dede Hermawan, Pradita Wuri Safitri, Ananda Sujati, Yuyut Prayuti, and Arman Lany. "Perception and Practices of Health Data Privacy Protection among Consumers: An Empirical Study in One of Indonesia's Major Cities." *Jurnal Indonesia Sosial Teknologi* 5, no. 6 (2024): 2795 - 2802

[6] Ahdiana Yuni Lestari, Misran Misran, Trisno Raharjo, Muhammad Annas, Dinda Riskanita, and Adya Paramita Prabandari. Meningkatkan Keamanan Data Pasien Layanan Kesehatan: Model Kerangka Kerja Terpadu untuk Rekam Medis Elektronik dari Perspektif Hukum. *Law Reform* 20, no. 2 (2024): 329-352. https://doi.org/10.14710/lr.v20i2.56986

BACARITA Law Journal, 6 (2) April 2026: 290 - 304
E-ISSN: 2775-9407
Published by: Program Study of Law Outside the Main Campus, Universitas Pattimura, Dobo, Indonesia.

	tata kelola dan & mekanisme E-Healt	
Analisis Aspek Keamanan Informasi Data Pasien Pada Rekam Medis Elektronik Di UPT Puskesmas Karangploso	Dalam jurnal ini membahas tentang praktik teknis dan manajemen informasi sedangkan dalam penelitian yang dilakukan berorientasi pada regulasi dan tata kelola hukum	Dari dua penelitian ini sama-sama membahas keamanan data kesehatan dan perlindungan informasi pasien dalam sistem digital
Analisis Yuridis Kebocoran Data di Layanan Kesehatan Digital: Studi Kasus Aplikasi Telemedicine di Indonesia	Sama-sama berfokus pada perlindungan data pribadi di sektor kesehatan digitaln dengan tujuan untuk melindungi data pasien dan mendorong penerapan UU PDP.	Dalam penelitian yang dilakukan menekankan bahwa pencegahan melalui tatakelola E-Healt sedangkan dalam jurnal ini menekankan penegakan hukum pasca-insiden.

Pada sistem *E-health* memiliki tingkat kepentingan yang sangat tinggi, mengingat data kesehatan termasuk informasi yang sangat rentan dan memerlukan perlindungan khusus dari akses tidak sah serta risiko kebocoran. Pengelolaan yang efektif menjamin kerahasiaan, integritas, dan ketersediaan data pasien, dengan memastikan bahwa hanya otoritas berwenang yang dapat mengakses informasi tersebut; data tidak dapat diubah tanpa izin; serta informasi tersedia saat dibutuhkan, dengan pendekatan pengelolaan yang baik, potensi gangguan operasional, kebocoran data pasien, dan ketidakpatuhan terhadap pengobatan kesehatan dapat dikurangi. Demikian pengelolaan keamanan data kesehatan dalam sistem E-health menjadi elemen mendasar dalam melindungi informasi sensitif serta kunci untuk menjaga kualitas layanan kesehatan digital yang modern dan terintegrasi.

Seiring dengan pentingnya penguatan tata kelola keamanan data dalam sistem E-Health, penelitian ini diarahkan untuk mengkaji beberapa permasalahan pokok. Pertama, bagaimana penerapan prinsip-prinsip perlindungan data pribadi dalam tata kelola keamanan data kesehatan pada sistem e-Health di Indonesia. Ketiga, apa saja tantangan dan solusi yang dihadapi dalam implementasi perlindungan data pribadi pada tata kelola keamanan data kesehatan di Indonesia. Rumusan masalah ini menjadi landasan analisis dalam penelitian serta menegaskan pentingnya evaluasi komprehensif terhadap sistem perlindungan data kesehatan di era digital.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan dua pendekatan, yaitu pendekatan konseptual dan pendekatan perundang-undangan. Pendekatan konseptual digunakan untuk memperdalam pemahaman atas konsep-konsep utama terkait perlindungan data pribadi, keamanan informasi, dan tata kelola *e-Health*. Sementara itu, pendekatan perundang-undangan digunakan untuk menelaah kerangka regulasi yang mengatur isu tersebut. Kedua pendekatan ini sejalan dengan karakter penelitian hukum normatif yang berfokus pada analisis terhadap norma, doktrin, dan literatur hukum yang relevan.[7]

[7] Rusdin Tahir, I Gede Pantja Astawa, Agus Widjajanto, Mompang L Panggabean, Moh Mujibur Rohman, Ni Putu Paramita Dewi, Nandang Alamsah Deliarnoor, Muhamad Abas, Rizqa Febry Ayu, Ni Putu Suci Meinarni, Fatimah Hs, Ni Wayan Eka Sumartini, Dewi

BACARITA Law Journal, 6 (2) April 2026: 290 - 304
E-ISSN: 2775-9407
Published by: Program Study of Law Outside the Main Campus, Universitas Pattimura, Dobo, Indonesia.

HASIL DAN PEMBAHASAN

A. Prinsip Perlindungan Data Pribadi Diterapkan Dalam Tata Kelola Keamanan Data Kesehatan Pada Sistem E-Health Di Indonesia

Prinsip-Prinsip Perlindungan Privasi atas Data Pribadi dalam Program *E-Health* Perlindungan terhadap privasi data pribadi pasien dalam sistem *e-health* merupakan aspek krusial yang memerlukan pengaturan khusus, terutama terkait dengan tata cara pengumpulan dan pemrosesan data medis pasien dalam suatu basis data. Data tersebut harus dijaga agar tidak diungkapkan atau disebarluaskan tanpa sepengetahuan dan persetujuan pasien. Berdasarkan praktik di berbagai negara, perlindungan data pribadi idealnya diatur dalam suatu undang-undang khusus yang memuat prinsip-prinsip dasar perlindungan data. Salah satu ketentuan pokoknya adalah bahwa data medis pasien tidak boleh dikumpulkan tanpa adanya persetujuan eksplisit dari pasien, serta pengumpulan dan pemrosesan data tersebut harus dilakukan sesuai dengan tujuan awal pengumpulannya.

Sebagai contoh, apabila data medis dikumpulkan dan diproses untuk kepentingan pengobatan di rumah sakit, maka data tersebut tidak boleh digunakan kembali oleh pihak lain, seperti perusahaan asuransi atau industri farmasi, setelah pengobatan selesai. Selain itu, pasien memiliki hak untuk mengetahui tujuan pengumpulan data pribadinya. Prinsip lainnya menekankan pentingnya jaminan keamanan sistem dari penyedia layanan kesehatan agar tidak terjadi kehilangan, kebocoran, pencurian, maupun akses ilegal terhadap data medis yang disimpan. Secara umum, prinsip-prinsip utama perlindungan privasi atas data pribadi dalam program e-health meliputi beberapa aspek berikut:

a. Prinsip Kesepakatan (*Consent Principle*)

Pasien sebagai pemilik data kesehatan berhak memberikan atau menolak persetujuan atas penggunaan datanya, kecuali dalam kondisi: 1) terdapat izin tertulis dari pasien sebagai pemilik data; 2) terdapat perintah berdasarkan undang-undang; atau 3) penggunaan data dilakukan untuk kepentingan pasien itu sendiri. Prinsip Kesepakatan (*Consent Principle*) menjadi landasan utama dalam perlindungan data kesehatan karena dalam asas ini menegaskan bahwa yang mana otonomi pasien sebagai pemilik data, khusunya terkait hak dalam mengontrol dan membuat keputusan terkait pemrosesan data kesehatannya. Etika medis dan perlindungan data pribadi, *consent* dipahami sebagai bentuk kontrol pasian terhadap persetujuan atau izin terhadap suatu tindakan medis atau penggunaan data pribadi mereka. Hal tersebut mencerminkan prinsip otonomi, kerahasiaan, serta hak atas privasi yang telah lama menjadi pilar hubungan dokter dan pasien. Seperti contohnya dalam konsep kepemilikan pasien atas isi rekam medis mengandung pengakuan bahwa pasien memiliki hak eksklusif dalam menentukan bagaimana datanya dipergunakan, termasuk memberikan izin ataupun menolak izin akses terhadap pihak lain.[8] Sehingga, kesepakatan bukan hanya dalam prosedur administrasi, akan tetapi meruspakan suatu mekanisme hukum yang melindungi kedali penuh pasian atas data pribadinya.

Namun dalam kondisi tertentu, pengiriman atau penggunaan data pasien tidak memerlukan persetujuan dari pasien. Dari pengecualian tersebut dianggap sah sepanjang

---

Kania Sugiharti, Saptaning Ruju Paminto. *Metodologi Penelitian Bidang Hukum: Suatu Pendekatan Teori Dan Praktik*. (Jambi: Sonpedia Publishing Indonesia, 2023).

[8] Anggra Yudha Ramadianto. "Hak Milik Pasien Atas Isi Rekam Medis (Suatu Pendekatan Filosofis Dan Hukum Perdata)." *Simbur Cahaya* (2019): 131-158. https://doi.org/10.28946/sc.v26i2.538.

BACARITA Law Journal, 6 (2) April 2026: 290 - 304
E-ISSN: 2775-9407
Published by: Program Study of Law Outside the Main Campus, Universitas Pattimura, Dobo, Indonesia.

memenuhi prinsip proporsionalitas serta memberikan perlindungan maksimal terhadap hak pasien. Contohnya, perintah undang-undang dapat diterapkan dalam konteks surveilans kesehatan, investigasi epidemiologi, atau kewajiban pelaporan penyakit tertentu, dengan tetap menjaga kerahasiaan data sesuai ketentuan dalam Peraturan Menteri Kesehatan mengenai rekam medis elektronik. Sistem rekam medis elektronik, setiap institusi kesehatan wajib unruk menerapkan mekaniasme teknis yang menjamin keamanan data pasian serta memberikan akses terbatas berdasarkan kebutuhan layanan, hal ini bertujuan agar adanya pengecualian tidak menjadi celah bagi penyalahgunaan data.[9] Demikian, meskipun pengecualian diperkenankan, penggunaannya harus memiliki batasan yang ketat dan senantiasa mengutamakan perlindungan terhadap hak pasien.

Pelaksanaan prinsip ini, tantangan terbesar terletak pada penerapan prinsip *consent* ini dalam sistem E-health yang semakin kompleks. Diperlukan kepastian norma hukum, peningkatan literasi pasien, serta kesiapan teknologi informasi kesehatan agar persetujuan dapat diberikan secara sadar (informed), bersifat dapat dicabut, dan dapat secara audit. Tanpa adanya sistem manajemen *consent* yang kokoh, peningkatan risiko akses tanpa izin, mengungkapkan data yang tidak sesuai, serta memproses data tanpa dasar hukum semakin mengancam. Oleh karena itu, penerapan prinsip *consent* harus dilengkapi dengan mekanisme transparansi, akuntabilitas, dan pengawasan yang tegas agar hak pasien sebagai pemilik data terlindungi secara optimal baik dari segi hukum maupun etika.

b. Prinsip Tujuan Spesifik (*Purpose Limitation Principle*)

Prinsip tujuan khusus (*purpose specification principle*) menegaskan bahwa setiap pengumpulan data harus memiliki tujuan yang jelas dan spesifik. Penggunaan data selanjutnya wajib dibatasi hanya untuk tujuan yang telah ditentukan sejak awal. Pelanggaran terhadap prinsip ini terjadi apabila data dipakai untuk kepentingan lain di luar tujuan pengumpulan awal tanpa persetujuan tambahan dari pemilik data.[10] Prinsip tersebut menjadi penting karena perlindungan data pribadi merupakan bagian dari hak asasi manusia yang dijamin oleh konstitusi, khususnya sebagai bentuk perlindungan diri pribadi dalam Pasal 28G ayat (1) UUD 1945. Fenomena penyalahgunaan data pribadi di Indonesia, seperti praktik jual beli data konsumen dan penipuan berbasis data, menunjukkan pelanggaran nyata terhadap prinsip tujuan khusus. Data yang pada awalnya diberikan untuk kepentingan transaksi atau layanan justru dialihkan untuk tujuan komersial lain tanpa sepengetahuan maupun persetujuan subjek data. Hal ini membuktikan bahwa pengumpulan data di Indonesia sering kali tidak disertai pembatasan yang tegas mengenai tujuan penggunaan dan larangan penggunaan ulang data di luar konteks pengumpulan. Undang-Undang Perlindungan Data Pribadi (Undang-Undang PDP) hadir sebagai kemajuan dalam memberikan pengakuan hak subjek data serta penetapan sanksi atas pelanggaran penggunaan data, penerapannya masih menghadapi hambatan struktural yang berpengaruh terhadap efektivitas pelaksanaan prinsip tujuan khusus. Undang-Undang PDP belum merinci pengaturan terkait mekanisme pembatasan tujuan, prosedur perubahan tujuan penggunaan data, dan standar pengujian kesesuaian tujuan (*compatibility test*). Selain itu, belum terbentuknya otoritas pengawas independen serta terbatasnya kapasitas lembaga pelaksana dan rendahnya literasi digital menjadikan prinsip pembatasan

[9] Jaka Kusnanta Wahyuntara, Endang Wahyati Yustina, and Dodik Tugasworo. "Pelindungan Hak atas Rahasia Medis Pasien dalam Implementasi Rekam Medis Elektronik (Studi pada Rumah Sakit Bhayangkara, Semarang)." *Soepra Jurnal Hukum Kesehatan* 10, no. 1 (2024): 158-175. https://doi.org/10.24167/sjhk.v10i1.11498.

[10] Sinta Dewi Rosadi, *Op. Cit.*

BACARITA Law Journal, 6 (2) April 2026: 290 - 304
E-ISSN: 2775-9407
Published by: Program Study of Law Outside the Main Campus, Universitas Pattimura, Dobo, Indonesia.

tujuan sulit ditegakkan secara operasional. prinsip tujuan khusus secara normatif telah menjadi bagian dari mandat konstitusional perlindungan data pribadi, namun secara empiris masih lemah penegakannya karena ketiadaan perangkat teknis yang memastikan bahwa data tidak digunakan melebihi tujuan awal pengumpulannya. Oleh karena itu, harmonisasi lebih lanjut dengan standar internasional serta pembentukan otoritas pengawas independen menjadi langkah krusial untuk menutup celah pelanggaran prinsip tujuan khusus dalam praktik perlindungan data di Indonesia.[11]

c. Prinsip Keamanan (*Security Principle*)

Pihak yang menggunakan atau menyimpan data wajib mengambil langkah-langkah yang diperlukan untuk menjaga keamanan data, termasuk melindunginya dari gangguan, kebocoran, maupun akses tidak sah dari pihak lain. Sistem e-health, keamanan menjadi aspek yang sangat penting mengingat nilai data kesehatan yang tinggi serta tingginya risiko serangan siber terhadap fasilitas kesehatan. Bidang kesehatan adalah salah satu sektor paling rentan terhadap kebocoran data akibat kombinasi faktor kompleksitas sistem, kesalahan manusia, dan penggunaan teknologi lama. Maka dari itu, penyelenggaraan sistem diwajibkan untuk menerapkan lapisan pengamanan yang komprehensif, seperti kontrol akses, enkripsi, dan audit. Pertama, mekanisme kontrol akses berupa penggunaan kata sandi, PIN, atau autentikasi berbasis peran, membatasi akses hanya untuk pihak yang berwenang terhadap data sensitive, dalam satu artikel menyebutkan bahwa sistem RME wajib mencatat jejak aktivitas (*audit trail*) untuk mengidentifikasi siapa yang mengakses, mengubah, atau menghapus data serta waktu pelaksanaannya.[12] Kedua, teknologi enkripsi berperan penting dalam melindungi data pasien yang tersimpan, misalnya dengan penerapan algoritme AES dalam tata kelola rekam medis berbasis teknologi informasi di Indonesia, sehingga kerahasiaan data dapat terjamin.[13] Ketiga, audit sistem secara berkelanjutan diperlukan agar setiap akses dapat direkam dan dievaluasi kembali guna memastikan akuntabilitas dan mencegah pelanggaran keamanan. Penerapan ketiga mekanisme ini tidak hanya memperkuat pelaksanaan prinsip retensi dengan aman, ttapi juga mencerminkan praktik keamanan terbaik yang dianjurkan dalam kebijakan regulasi Kesehatan, dengan menggabungkan langkah-langkah teknis, prinsip keamanan dapat diimplementasikan secara efektif sehingga risiko gangguan, kebocoran, dan akses tidak sah terhadap data pasien dapat diminimalisasi.

d. Prinsip Retensi (*Retention Principle*)

Prinsip ini mengatur jangka waktu penyimpanan data. Setelah data digunakan sesuai dengan tujuan pengumpulannya, data tersebut harus segera dimusnahkan untuk mencegah penyalahgunaan di masa mendatang. Selain prinsip-prinsip tersebut, penyelenggara sistem *e-health* juga wajib menerapkan standar keamanan data pribadi pasien, antara lain dengan: 1) menyediakan mekanisme kontrol akses seperti penggunaan kata sandi (*password*) dan nomor identifikasi pribadi (PIN) agar akses terhadap data pasien terbatas hanya pada pihak yang berwenang; 2) menerapkan teknologi enkripsi dalam

[11] Gunawan Karnedi, and RG Guntur. Alam. "Evaluasi Regulasi Perlindungan Data Pribadi di Indonesia: Komparasi dengan GDPR Uni Eropa." *El-Mujtama: Jurnal Pengabdian. Masyarakat* 5, no. 3 (2025): 610 - 622. https://doi.org/10.47467/elmujtama.v5i3.8549.

[12] Amelinda Helsa Meilani, Sri Wahyuningsih Nugraheni, and Budi Suprawita. "Analisis Implementasi Rekam Medis Elektronik Terhadap Mutu Pelayanan Rawat Jalan di Rsud Ibu Fatmawati Soekarno Kota Surakarta". *Infokes: Jurnal Ilmiah Rekam Medis dan Informatika Kesehatan* 15, no. 2 (2025): 158-164. https://doi.org/10.47701/4b9q1c44.

[13] Aellen Sarce Joel, Falaah Abdussalaam, and Yuyun Yunengsih. "Tata Kelola Rekam Medis Berbasis Teknologi Informasi dalam Penanganan Kerahasiaan dan Keamanan Data Pasien dengan Metode Kriptografi." *Jurnal Indonesia: Manajemen Informatika dan Komunikasi* 4, no. 3 (2023): 837-848. ttps://doi.org/10.35870/jimik.v4i3.287.

BACARITA Law Journal, 6 (2) April 2026: 290 - 304
E-ISSN: 2775-9407
Published by: Program Study of Law Outside the Main Campus, Universitas Pattimura, Dobo, Indonesia.

penyimpanan data agar informasi pribadi pasien tidak dapat diakses oleh pihak tidak berwenang; dan 3) melaksanakan audit sistem yang dapat merekam aktivitas akses terhadap data kesehatan untuk memastikan akuntabilitas serta mencegah pelanggaran privasi.[14]

Pada prinsip ini menekankan bahwa sangat penting untuk menjaga privasi pasien, karena apabila menumpuknya data pasien yang sudah tidak digunakan dapat menimbulkan resiko terhadap keamanan informasi. Di banyak fasilitas yang menggunakan sistem elektronik, banyak yang belum menyediakan kebijakan pemusnahan data yang secara tegas dan konsisten. Contohnya, analisis terhadap aspek keamanan data di Rumah Sakit X menunjukkan bahwa meskipun akses data dilengkapi dengan autentikasi, belum ada prosedur operasional standar untuk pemusnahan data secara berkala, namun ada regulasi internal yang mengatur hal ini secara bertahap.[15] Selain itu, dari sisi regulasi, sistem e-health harus selaras dengan peraturan perlindungan data pasien, dengan penerapan retensi data yang tepat, penyelenggara dapat menyeimbangkan kebutuhan untuk mempertahankan data penting, misalnya untuk audit, penelitian, atau pertanggungjawaban klinis, dengan kewajiban etis dan hukum dalam menjaga privasi pasien.

B. Tantangan dan Solusi yang Dihadapi Dalam Penerapan Perlindungan Data Pribadi pada Tata Kelola Keamanan Data Kesehatan di Indonesia

Negara khususnya Indonesia, bertanggung jawab dalam merumuskan aturan yang melindungi data kesehatan. Negara-negara tetap memiliki kewajiban untuk mengelola dan memastikan penerapan kebijakan serta standar yang harus diikuti oleh penyedia layanan kesehatan, agar data pasien tetap aman. Aturan ini tidak hanya perlu dibuat secara formal, tetapi juga harus dilengkapi dengan sistem hukum yang jelas untuk memberikan sanksi jika terjadi pelanggaran. Secara umum, negara-negara meningkatkan standar keamanan dengan aturan yang ketat serta menyediakan mekanisme pengawasan dan sanksi untuk mengurangi risiko kebocoran data pasien.[16] Contohnya dalam Kasus kebocoran data BPJS 2021: Kasus kebocoran data pribadi peserta BPJS Kesehatan pada tahun 2021 menjadi salah satu contoh paling signifikan mengenai lemahnya sistem perlindungan data di Indonesia sebelum hadirnya kerangka hukum yang komprehensif. Pada masa itu, Indonesia belum memiliki Undang-Undang Perlindungan Data Pribadi (Undang-Undang PDP), sehingga penanganan insiden dilakukan dengan mengandalkan Undang-Undang Informasi dan Transaksi Elektronik (Undang-Undang ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Peraturan Pemerintah PSTE), serta Permenkominfo Nomor 20 Tahun 2016. Regulasi tersebut sifatnya masih parsial dan lebih menekankan pada aspek penindakan setelah terjadi pelanggaran (reaktif), bukan pada pencegahan.

Respons pemerintah dalam kasus BPJS Kesehatan, dilakukan melalui langkah-langkah seperti audit digital oleh Kementerian Kominfo, investigasi kepolisian, serta koordinasi dengan Badan Siber dan Sandi Negara (BSSN). Namun perangkat hukum yang berlaku

[14] Sinta Dewi Rosadi, *Op. Cit.*

[15] Efri Tri Ardianto, Sabran, and Lensa Nurjanah. "Analisis aspek keamanan data pasien dalam implementasi rekam medis elektronik di Rumah Sakit X." *Jurnal Rekam Medik Dan Manajemen Informasi Kesehatan* 3, no. 2 (2024): 18-30. https://doi.org/10.47134/rmik.v3i2.54.

[16] Nahlda Zahrani Balqish, and Atika Puspita Marzaman. "Peran Keamanan Siber dalam Melindungi Data Kesehatan: Tanggung Jawab Negara dan Lembaga Internasional dalam Era Digital." *Triwikrama: Jurnal Ilmu Sosial* 8, no. 6 (2025): 131-140. https://doi.org/10.9963/a0f5x575

BACARITA Law Journal, 6 (2) April 2026: 290 - 304
E-ISSN: 2775-9407
Published by: Program Study of Law Outside the Main Campus, Universitas Pattimura, Dobo, Indonesia.

pada saat itu belum mengatur secara terstruktur mengenai mekanisme pencegahan, kewajiban notifikasi kepada subjek data, serta bentuk sanksi administratif yang spesifik bagi pengendali data seperti BPJS. Ketiadaan regulasi yang lengkap ini memperlihatkan adanya kekosongan hukum terutama dalam aspek perlindungan preventif terhadap hak-hak subjek data.

Sebelum berlakunya Undang-Undang PDP, penyelesaian sengketa atau kasus kebocoran data pribadi sepenuhnya bergantung pada Undang-Undang ITE sebagai dasar hukum utama. Undang-undang ini hanya mengatur satu ketentuan eksplisit mengenai data pribadi, yaitu Pasal 26 ayat (1) yang menegaskan bahwa penggunaan data pribadi seseorang harus seizin pemilik data. Namun Undang-Undang ITE tidak mengatur klasifikasi data pribadi, kewajiban rinci bagi pengendali data, hak-hak subjek data, maupun mekanisme remedial bagi korban. Selain itu, tidak terdapat lembaga pengawas khusus yang bertugas menangani insiden kebocoran data secara sistematis dan berkesinambungan. Akibatnya, perlindungan hukum yang diberikan lebih bersifat represif, yaitu hanya hadir setelah pelanggaran terjadi.

Berbeda dengan kondisi tersebut, hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Undang-Undang PDP) membawa pendekatan yang jauh lebih komprehensif dan terstruktur. UU ini tidak hanya menyediakan mekanisme penegakan hukum, tetapi juga mengatur secara jelas upaya pencegahan melalui prinsip-prinsip pengolahan data pribadi, seperti hak untuk mengetahui, mengakses, memperbaiki, menghapus, serta menarik persetujuan sebagaimana tercantum dalam Pasal 5. Selain itu, Pasal 13 mengatur persyaratan sahnya persetujuan dalam pengolahan data pribadi, sementara Pasal 14 menegaskan kewajiban dan standar pengolahan data oleh pengendali maupun prosesor data. Kehadiran Undang-Undang PDP, pengelolaan data pribadi di Indonesia memperoleh dasar hukum yang konsisten, komprehensif, serta menempatkan hak subjek data sebagai pusat pengaturannya.[17]

Perlindungan data pribadi di Indonesia semakin menjadi perhatian karena berkembangnya teknologi informasi dan komunikasi. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Undang-Undang PDP) diharapkan bisa memberikan pedoman hukum yang jelas untuk melindungi hak orang-orang terkait data pribadinya. Namun, dalam menerapkan hukum perlindungan data pribadi di Indonesia masih ada berbagai tantangan. Salah satu tantangan besar adalah kurangnya kesadaran masyarakat tentang hak-hak mereka terkait data pribadi. Selain itu, lembaga penegak hukum juga mengalami keterbatasan dalam sumber daya, sehingga sulit menangani kasus pelanggaran data secara efektif. Hal ini semakin sulit karena aturan yang ada terkadang cukup rumit dan masih memerlukan penjelasan lebih lanjut agar bisa dijalankan dengan baik. Di bagian ini, kita akan membahas secara rinci setiap tantangan yang muncul, yaitu sebagai berikut:

(1) Kurangnya Kesadaran Masyarakat

Salah satu masalah besar dalam menerapkan hukum perlindungan data pribadi adalah masyarakat masih kurang memahami hak-hak mereka. Karena ini, banyak orang tidak melaporkan ketika data pribadinya dirugikan, dengan kurang kesaadaran dari masyarakat

[17] Rita Alfiana, and Nita Nur Aisyah. "Perlindungan Hukum Terhadap Data Pribadi Pasca Undang-Undang Data Pribadi Nomor 27 Tahun 2022 (Studi Kasus BPJS Kesehatan)". *Arus Jurnal Sosial dan Humaniora* 5, no. 2 (2025): 2724-2731.

BACARITA Law Journal, 6 (2) April 2026: 290 - 304
E-ISSN: 2775-9407
Published by: Program Study of Law Outside the Main Campus, Universitas Pattimura, Dobo, Indonesia.

ini cukup menghambat asas yang dianut dalam Undang-Undang PDP yaitu asas *complaint-based enforcement.* Masyarakat dalam kondisi yang baik, yang dirugikan harus bisa mengidentifikasi bentuk pelanggaran, serta memahami mekanis pelaporan. Di Indonesia masih banyak ditemukan, masyarakat yang mengaku perhatian terhadap privasi akan tetapi tetap membagi data tersebut secara luas. Sikap ini muncul karena kurangnya pemahanan masyarakat terhadap resiko kebocoran data, ketidakjelasan definisi data pribadi, serta minimnya edukasi yang diselenggarakan oleh pemerintah maupun sektok swasta. Contohnya, dalam Pasal 26 Undang-Undang PDP disebutkan bahwa setiap orang memiliki hak untuk mengetahui bagaimana data pribadinya digunakan. Namun, jika masyarakat tidak mengerti hak ini, mereka tidak akan bertindak untuk melindungi data pribadinya.

(2) Keterbatasan Sumber Daya Penegak Hukum

Pelanggaran terhadap data pribadi kerap menjadi kejahatan yang berkaitan dengan teknologi dan memerlukan seseorang yang ahli dalam bidang digital, pemahaman yang mendalam terhadap sistem informasi, serta mempuan analisis terhadap kerentanan kemanan. Namun masalah lain yang juga sangat penting adalah keterbatasan sumber daya yang dimiliki oleh instansi penegak hukum. Banyak lembaga belum memiliki kemampuan yang cukup untuk menangani kasus pelanggaran data secara baik. Hal ini bisa terjadi karena jumlah pegawai yang telah terlatih dalam bidang data tidak cukup, serta dana yang dialokasikan untuk penegakan hukum masih terbatas. Pasal 45 Undang-Undang PDP, berlaku sanksi administratif terhadap pelanggar, tetapi tanpa sumber daya yang memadai, hukuman ini sulit diterapkan. Adapun dampak dari keterbatasan sumber daya penegak hukum adalah b anyak laporan tidak diproses karena kekurangan kapasitas investigasi serta sanksi administratif Pasal 45 sering tidak diterapkan.

(3) Kompleksitas Regulasi

Kompleksitas aturan juga menjadi penghalang dalam penerapan hukum perlindungan data pribadi. Beberapa ketentuan dalam Undang-Undang PDP masih perlu jelas agar bisa diterapkan dengan tepat. Misalnya, di Pasal 14 Undang-Undang PDP disebutkan bahwa setiap orang harus memberi persetujuan sebelum data pribadinya digunakan. Namun, definisi dan cara memberi persetujuan masih perlu dijelaskan dengan lebih rinci agar tidak ada penafsiran yang berbeda. Selain itu, terdapat tumpang tindih antara Undang-Undang PDP dengan undang-undang lain seperti Undang-Undang ITE dan Undang-Undang Perlindungan Konsumen. Hal ini bisa menyebabkan kesulitan dalam menerapkan hukum, karena pelanggaran data bisa dianggap berbeda oleh berbagai lembaga.

(4) Tindak Lanjut yang Tidak Memadai

Tindak lanjut atas pelanggaran data pribadi yang dilaporkan juga menjadi isu yang penting. Meskipun Undang-Undang Perlindungan Data Pribadi memberikan dasar hukum yang jelas, pelaksanaannya di lapangan sering tidak sesuai dengan harapan. Banyak laporan pelanggaran data tak ditangani secara serius oleh lembaga hukum, sehingga membuat masyarakat tak puas. Data dari Kominfo menunjukkan bahwa dari lebih dari 1.000 laporan pelanggaran, hanya sekitar 20% yang mendapat tindak lanjut yang memadai. Ini menunjukkan perbedaan antara harapan masyarakat dan kenyataan dalam penegakan hukum. Pasal 46 Undang-Undang PDP dijelaskan bahwa lembaga wajib melakukan

BACARITA Law Journal, 6 (2) April 2026: 290 - 304
E-ISSN: 2775-9407
Published by: Program Study of Law Outside the Main Campus, Universitas Pattimura, Dobo, Indonesia.

investigasi terhadap pelaporan pelanggaran, tetapi tanpa mekanisme yang jelas dan dukungan resource yang memadai, banyak laporan terabaikan.

(5) Peran Sektor Swasta

Sektor swasta juga punya peran penting dalam memastikan perlindungan data pribadi. Banyak perusahaan mengumpulkan dan memproses data pribadi, tapi tidak semua mengikuti ketentuan Undang-Undang PDP. Pasal 15 Undang-Undang PDP dijelaskan bahwa pengendali data wajib melindungi data pribadi yang mereka olah. Namun, masih banyak perusahaan yang belum menerapkan metode terbaik dalam menjaga data pribadi.

(6) Ketidakpastian Hukum

Ketidakpastian hukum juga menjadi tantangan dalam penegakan perlindungan data pribadi. Banyak pihak merasa bingung mengenai batasan dan konsekuensi dari pelanggaran data. Hal ini diperparah karena kurangnya contoh hukum yang jelas terkait pelanggaran data di Indonesia. Adapun dampak dalam hal ini yaitu penegakan sanksi pidana tidak konsisten, korban tidak mengetahui jalur hukum yang harus ditempuh. Pasal 47 Undang-Undang PDP juga dijelaskan sanksi pidana bagi pelanggar, tetapi penerapan sanksi tersebut masih belum konsisten.

(7) Perkembangan Teknologi yang Cepat

Perkembangan teknologi yang sangat cepat menjadi tantangan dalam menjaga perlindungan data pribadi. Teknologi baru seperti blockchain, big data, dan internet of things membuat cara pengolahan dan penyimpanan data pribadi semakin rumit. Hal ini membuat aturan yang ada sulit diadaptkan secara cepat. Pasal 5 Undang-Undang PDP dijelaskan prinsip-prinsip pengolahan data pribadi, tetapi prinsip ini perlu diperbarui agar sesuai dengan perkembangan teknologi terbaru.[18]

Perlindungan data pribadi dan privasi sangat penting dalam bidang kesehatan agar informasi kesehatan seseorang tetap rahasia dan aman. Informasi seperti riwayat sakit dan keadaan kesehatan seseorang termasuk data yang sensitif, sehingga perlu dilindungi dari akses yang tidak berhak dan penyalahgunaan. Data kesehatan juga bisa terkena ancaman dari dunia maya, sehingga bisa bocor atau disalahgunakan. Oleh karena itu, perlindungan yang baik dan tepat sangat penting untuk mencegah kebocoran data dan menjaga hak privasi pasien. Kepatuhan terhadap peraturan yang berlaku seperti Undang-Undang Perlindungan Data Pribadi (Undang-Undang PDP), Undang-Undang Kesehatan, dan Peraturan Menteri Kesehatan tentang rekam medis sangat penting untuk menjaga kerahasiaan dan keamanan data pasien. Penyedia layanan kesehatan seperti rumah sakit, puskesmas, klinik, dan tenaga medis harus menerapkan langkah keamanan yang tepat seperti enkripsi data serta memberikan pelatihan kepada staf agar pengelolaan data tetap aman dan sesuai. Menurut kemenkes ada beberapa solusi dalam mengatasi masalah dan risiko yang ada, diperlukan beberapa solusi yang lengkap dan mendalam.

(1) Penggunaan teknologi enkripsi yang baik serta sistem kontrol akses yang membatasi hak pengguna harus menjadi prioritas utama dalam setiap sistem informasi kesehatan. Menggunakan firewall yang lebih canggih dan metode autentikasi dengan beberapa faktor,

[18] Randy Artawijaya, and Sidi Ahyar Wiraguna. "Tantangan Penegakan Hukum Dalam Pelindungan Data Pribadi Perspektif Undang-Undang No. 27 Tahun 2022". *Jurnal Ilmiah Kajian Multidisipliner* 9, no. 5 (2025): 231–239. https://sejurnal.com/pub/index.php/jikm/article/view/6296

BACARITA Law Journal, 6 (2) April 2026: 290 - 304
E-ISSN: 2775-9407
Published by: Program Study of Law Outside the Main Campus, Universitas Pattimura, Dobo, Indonesia.

seperti SMS atau kode rahasia, bisa membuat data lebih aman terhadap serangan dari internet.

(2) Lembaga yang menangani data kesehatan harus menyusun kebijakan privasi yang jelas. Kebijakan ini harus menjelaskan cara data dikumpulkan, disimpan, dan digunakan. Selain itu, petugas kesehatan dan staf di bagian administrasi perlu diberi pelatihan rutin mengenai cara menjaga kerahasiaan data dan mengikuti kebijakan privasi. Hal ini bisa membuat mereka lebih paham dan patuh terhadap aturan yang berlaku. Juga, audit dan pemeriksaan keamanan secara berkala sangat penting, karena bisa memastikan sistem tetap aman sesuai dengan standar yang berlaku. Teknologi seperti kecerdasan buatan (AI) dan pembelajaran mesin (*machine learning*) juga bisa digunakan untuk mendeteksi kegiatan mencurigakan atau perubahan tidak wajar dalam data secara langsung, sehingga memberikan perlindungan tambahan.

(3) Untuk menjaga keamanan data secara berkelanjutan, perlu diikuti aturan-aturan global seperti GDPR dan HIPAA yang bisa menjadi pedoman dalam menjaga kualitas dan keselamatan data.

(4) Percepatan penerbitan peraturan pelaksana dan standar teknis yang rinci sangat penting agar ketentuan Undang-Undang PDP seperti definisi dan mekanisme pemberian persetujuan (consent) dapat diterapkan secara konsisten dan tidak multitafsir.[19]

(5) Kolaborasi antara pemerintah, lembaga kesehatan, dan perusahaan teknologi sangat penting agar tercipta lingkungan yang aman dan terlindungi. Dengan kerja sama ini, data kesehatan bisa digunakan secara aman untuk meningkatkan pelayanan kepada pasien tanpa mengorbankan privasi mereka.

(6) Penerapan *General Data Protection Regulation* (GDPR) di Eropa, Indonesia perlu melakukan analisis kesenjangan dan pengukuran kepatuhan terhadap regulasi yang ada. Adaptasi panduan teknis dan audit berkala di fasilitas kesehatan sangat penting untuk memastikan efektivitas perlindungan data medis. Selain itu, pembentukan tim khusus atau petugas perlindungan data (*Data Protection Officer*/DPO) di setiap institusi kesehatan dapat menjadi langkah strategis Kepercayaan pasien terhadap penyedia layanan kesehatan sangat bergantung pada keyakinan bahwa data mereka aman dan terlindungi. Pelanggaran terhadap privasi dapat menghambat pasien dalam memberikan informasi yang diperlukan untuk diagnosis dan pengobatan yang tepat. Oleh karena itu, perlindungan data medis bukan hanya soal kepatuhan hukum, tetapi juga membangun kepercayaan dan kualitas layanan Kesehatan.[20]

(7) Kepatuhan terhadap regulasi baik nasional seperti Undang-Undang Perlindungan Data Pribadi (Undang-Undang PDP), Undang-Undang Kesehatan, serta regulasi sektor lain dan standar global seperti GDPR dan HIPAA harus dijaga dan diawasi secara ketat. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Undang-Undang PDP), muncul sebagai langkah signifikan dalam sistem hukum Indonesia, bertujuan untuk menyediakan kerangka hukum yang lebih menyeluruh dan terpusat

[19] Muhamad Adri Rinjani, and Ricky Firmansyah. "Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia." *Jurnal Analisis Hukum* 8, no. 1 (2025): 70-83. https://doi.org/10.38043/jah.v8i1.6793

[20] Gunawan Widjaja, Hotmaria Hertawaty Sijabat, and Handojo Dhanudibroto. "Hak Pasien Atas Privasi Data Medis: Tinjauan Literatur Dan Evaluasi Kebijakan." *Zahra: Journal of Health and Medical Research* 5, no. 2 (2025): 12-22.

BACARITA Law Journal, 6 (2) April 2026: 290 - 304
E-ISSN: 2775-9407
Published by: Program Study of Law Outside the Main Campus, Universitas Pattimura, Dobo, Indonesia.

dalam mengatur hak-hak subjek data, kewajiban pengendali dan prosesor data, serta sanksi terhadap.[21]

KESIMPULAN

Penerapan prinsip-prinsip perlindungan data pribadi seperti kesepakatan, tujuan khusus, keamanan, dan retensi dalam tata kelola keamanan data kesehatan pada sistem e-Health di Indonesia masih menghadapi tantangan implementasi, meskipun didukung oleh Undang-Undang PDP Nomor 27 Tahun 2022. Prinsip kesepakatan menekankan mekanisme transparan dan auditabel untuk menjamin otonomi pasien, sementara keamanan memerlukan teknologi seperti enkripsi AES, kontrol akses berbasis peran, dan audit trail guna mencegah akses tidak sah. Kompleksitas regulasi, ketidakpastian hukum, keterbatasan sumber daya penegak hukum, serta rendahnya literasi masyarakat menjadi hambatan utama dalam penegakan perlindungan data kesehatan, ditambah kebocoran seperti kasus BPJS Kesehatan. Solusi mencakup percepatan peraturan pelaksana Undang-Undang PDP, harmonisasi dengan Undang-Undang ITE, penunjukan Data Protection Officer, pelatihan staf, dan adopsi standar global seperti GDPR untuk meningkatkan kapasitas pengawasan.

REFERENSI

Aellen Sarce Joel, Falaah Abdussalaam, and Yuyun Yunengsih. "Tata Kelola Rekam Medis Berbasis Teknologi Informasi dalam Penanganan Kerahasiaan dan Keamanan Data Pasien dengan Metode Kriptografi." *Jurnal Indonesia: Manajemen Informatika dan Komunikasi* 4, no. 3 (2023): 837-848. ttps://doi.org/10.35870/jimik.v4i3.287.

Ahdiana Yuni Lestari, Misran Misran, Trisno Raharjo, Muhammad Annas, Dinda Riskanita, and Adya Paramita Prabandari. Meningkatkan Keamanan Data Pasien Layanan Kesehatan: Model Kerangka Kerja Terpadu untuk Rekam Medis Elektronik dari Perspektif Hukum. *Law Reform* 20, no. 2 (2024): 329-352. https://doi.org/10.14710/lr.v20i2.56986.

Alaikha Annan. "Tinjauan Yuridis Perlindungan Data Pribadi Pada Sektor Kesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022". *Sinergi: Jurnal Ilmiah Multidisiplin* 1, no. 4 (2023): 247–254.

Amelinda Helsa Meilani, Sri Wahyuningsih Nugraheni, and Budi Suprawita. "Analisis Implementasi Rekam Medis Elektronik Terhadap Mutu Pelayanan Rawat Jalan di Rsud Ibu Fatmawati Soekarno Kota Surakarta". *Infokes: Jurnal Ilmiah Rekam Medis dan Informatika Kesehatan* 15, no. 2 (2025): 158-164. https://doi.org/10.47701/4b9q1c44.

Anggra Yudha Ramadianto. "Hak Milik Pasien Atas Isi Rekam Medis (Suatu Pendekatan Filosofis Dan Hukum Perdata)." *Simbur Cahaya* (2019): 131-158. https://doi.org/10.28946/sc.v26i2.538.

Efri Tri Ardianto, Sabran, and Lensa Nurjanah. "Analisis aspek keamanan data pasien dalam implementasi rekam medis elektronik di Rumah Sakit X." *Jurnal Rekam Medik*

[21] Predderics Hockop Simanjuntak. "Perlindungan Hukum Terhadap Data Pribadi Pada Era Digital di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi Dan General Data Protection Regulation (GDPR)." *Esensi Hukum* 6, no. 2 (2024): 105-124. https://doi.org/10.35586/esensihukum.v6i2.412.

Dan Manajemen Informasi Kesehatan 3, no. 2 (2024): 18-30. https://doi.org/10.47134/rmik.v3i2.54.

Gunawan Widjaja, Hotmaria Hertawaty Sijabat, and Handojo Dhanudibroto. "Hak Pasien Atas Privasi Data Medis: Tinjauan Literatur Dan Evaluasi Kebijakan." *Zahra: Journal of Health and Medical Research* 5, no. 2 (2025): 12-22.

Gunawan Karnedi, and RG Guntur. Alam. "Evaluasi Regulasi Perlindungan Data Pribadi di Indonesia: Komparasi dengan GDPR Uni Eropa." *El-Mujtama: Jurnal Pengabdian. Masyarakat* 5, no. 3 (2025): 610 - 622. https://doi.org/10.47467/elmujtama.v5i3.8549.

Handryas Prasetyo Utomo, Elisatris Gultom, and Anita Afriana. "Urgensi Perlindungan Hukum Data Pribadi Pasien dalam Pelayanan Kesehatan Berbasis Teknologi di Indonesia." *Jurnal Ilmiah Galuh Justisi* 8, no. 2 (2020): 168-185.

Indah Susilowati, Lia Agustina, and Ratna Frenty Nurkhalim. "Edukasi Mengenai Upaya Menjaga Privasi Data Pribadi Dalam Penggunaan E-Health." *Journal of Community Engagement and Empowerment* 7, no. 1 (2025): 63-69. https://www.ojs.iik.ac.id/index.php/JCEE/article/view/963.

Jaka Kusnanta Wahyuntara, Endang Wahyati Yustina, and Dodik Tugasworo. "Pelindungan Hak atas Rahasia Medis Pasien dalam Implementasi Rekam Medis Elektronik (Studi pada Rumah Sakit Bhayangkara, Semarang)." *Soepra Jurnal Hukum Kesehatan* 10, no. 1 (2024): 158-175. https://doi.org/10.24167/sjhk.v10i1.11498.

Joni Yusufa, Dede Hermawan, Pradita Wuri Safitri, Ananda Sujati, Yuyut Prayuti, and Arman Lany. "Perception and Practices of Health Data Privacy Protection among Consumers: An Empirical Study in One of Indonesia's Major Cities." *Jurnal Indonesia Sosial Teknologi* 5, no. 6 (2024): 2795 – 2802.

Muhamad Adri Rinjani, and Ricky Firmansyah. "Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia." *Jurnal Analisis Hukum* 8, no. 1 (2025): 70-83. https://doi.org/10.38043/jah.v8i1.6793.

Nahlda Zahrani Balqish, and Atika Puspita Marzaman. "Peran Keamanan Siber dalam Melindungi Data Kesehatan: Tanggung Jawab Negara dan Lembaga Internasional dalam Era Digital." *Triwikrama: Jurnal Ilmu Sosial* 8, no. 6 (2025): 131-140. https://doi.org/10.9963/a0f5x575.

Predderics Hockop Simanjuntak. "Perlindungan Hukum Terhadap Data Pribadi Pada Era Digital di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi Dan General Data Protection Regulation (GDPR)." *Esensi Hukum* 6, no. 2 (2024): 105-124. https://doi.org/10.35586/esensihukum.v6i2.412.

Randy Artawijaya, and Sidi Ahyar Wiraguna. "Tantangan Penegakan Hukum Dalam Pelindungan Data Pribadi Perspektif Undang-Undang No. 27 Tahun 2022". *Jurnal Ilmiah Kajian Multidisipliner* 9, no. 5 (2025): 231–239. https://sejurnal.com/pub/index.php/jikm/article/view/6296.

Rita Alfiana, and Nita Nur Aisyah. "Perlindungan Hukum Terhadap Data Pribadi Pasca Undang-Undang Data Pribadi Nomor 27 Tahun 2022 (Studi Kasus BPJS Kesehatan)". *Arus Jurnal Sosial dan Humaniora* 5, no. 2 (2025): 2724-2731.

Rusdin Tahir, I Gede Pantja Astawa, Agus Widjajanto, Mompang L Panggabean, Moh Mujibur Rohman, Ni Putu Paramita Dewi, Nandang Alamsah Deliarnoor, Muhamad Abas, Rizqa Febry Ayu, Ni Putu Suci Meinarni, Fatimah Hs, Ni Wayan Eka Sumartini, Dewi Kania Sugiharti, Saptaning Ruju Paminto. *Metodologi Penelitian Bidang Hukum: Suatu Pendekatan Teori Dan Praktik*. (Jambi: Sonpedia Publishing Indonesia, 2023).

Sinta Dewi Rosadi. "Implikasi Penerapan Program E-Health Dihubungkan Dengan Perlindungan Data Pribadi. Arena Hukum" 9, no. 3 (2016): 403-420. https://doi.org/10.21776/ub.arenahukum.2016.00903.6.

BACARITA Law Journal, 6 (2) April 2026: 290 - 304
E-ISSN: 2775-9407
Published by: Program Study of Law Outside the Main Campus, Universitas Pattimura, Dobo, Indonesia.