



Urgensi Pembentukan Regulasi Nasional Tentang Perlindungan Data Pasien Dalam Sistem Informasi Rumah Sakit

Mohammad Abdillah Napu¹, Rizky Isnanto Lahay², Tri Wibawa Putra T. Haras³

Fakultas Hukum, Universitas Negeri Gorontalo, Indonesia¹⁻³

Email Korespondensi: Abdinapu37@gmail.com, antholahay30@gmail.com, dhikyharss@gmail.com

Article received: 01 November 2025, Review process: 11 November 2025

Article Accepted: 25 Desember 2025, Article published: 05 Januari 2026

ABSTRACT

The development of digitalization in the health sector has transformed the governance of medical services through the implementation of hospital information systems and telemedicine services. This transformation has improved efficiency but also created risks to the protection of patients' personal data, which are sensitive and prone to misuse. This study aims to analyze the legal framework for patient data protection in Indonesia, assess the urgency of forming a comprehensive national regulation, and formulate the ideal regulatory direction in the digital era. The method used is normative juridical research with statutory and conceptual approaches. The results show that although several regulations exist – such as the Health Law, the Hospital Law, and the Personal Data Protection Law – they remain sectoral and do not provide comprehensive protection. Regulatory inconsistencies, weak law enforcement, limited infrastructure, and low digital literacy are the main obstacles. Therefore, a specific national regulation that is integrative, sets cybersecurity standards, governs patient data management, and clarifies the legal responsibilities of related parties is needed to ensure privacy rights and strengthen public trust in digital health services.

Keywords: Personal Data Protection; Privacy Rights; Hospitals; Progressive Law.

ABSTRAK

Perkembangan digitalisasi di sektor kesehatan telah mengubah tata kelola pelayanan medis melalui penerapan sistem informasi rumah sakit dan layanan telemedicine. Transformasi ini meningkatkan efisiensi, namun menimbulkan risiko terhadap perlindungan data pribadi pasien yang bersifat sensitif dan rawan disalahgunakan. Penelitian ini bertujuan menganalisis pengaturan hukum perlindungan data pasien di Indonesia, menilai urgensi pembentukan regulasi nasional yang komprehensif, serta merumuskan arah regulasi ideal di era digital. Metode yang digunakan adalah penelitian yuridis normatif dengan pendekatan perundang-undangan dan konseptual. Hasil penelitian menunjukkan bahwa meskipun telah ada beberapa peraturan seperti Undang-Undang Kesehatan, Rumah Sakit, dan Perlindungan Data Pribadi, seluruhnya masih bersifat sektoral dan belum memberikan perlindungan menyeluruh. Ketidaksinkronan antar regulasi, lemahnya penegakan hukum, keterbatasan infrastruktur, dan rendahnya literasi digital menjadi hambatan utama. Oleh karena itu, diperlukan regulasi nasional khusus yang bersifat integratif, menetapkan standar keamanan siber, mengatur tata kelola data pasien, serta memperjelas tanggung jawab hukum pihak terkait untuk menjamin hak privasi dan memperkuat kepercayaan publik terhadap layanan kesehatan digital.

Kata Kunci: Perlindungan Data Pribadi, Hak Privasi, Rumah Sakit, Hukum Progresif

PENDAHULUAN

Kesehatan merupakan hak asasi manusia dan salah satu unsur kesejahteraan yang harus diwujudkan sesuai dengan cita-cita Bangsa Indonesia yang tertera di dalam Undang-undang Dasar 1945 bahwa semua orang berhak sehat dan sejahtera. Setiap orang berhak atas taraf hidup yang memadai untuk kesehatan, kesejahteraan dirinya sendiri dan keluarga. Pasal 28 H ayat (1) Undang-Undang Dasar Republik Indonesia Tahun 1945 secara tegas menyatakan bahwa "Setiap orang berhak hidup sejahtera lahir dan batin, bertempat tinggal, dan mendapatkan lingkungan hidup yang baik dan sehat serta berhak memperoleh pelayanan kesehatan."

Salah satu wujud nyata dari tanggung jawab negara dalam memberikan layanan kesehatan adalah dengan menyediakan fasilitas pelayanan kesehatan seperti rumah sakit, puskesmas, klinik, dan bentuk pelayanan kesehatan lainnya. Keberadaan fasilitas ini menjadi instrumen penting dalam menjamin bahwa masyarakat dapat dengan mudah mengakses layanan kesehatan, baik yang bersifat promotif, preventif, kuratif, maupun rehabilitatif.

Digitalisasi kesehatan adalah peralihan atau transformasi di bidang kesehatan yang bertujuan untuk membantu fasilitas pelayanan kesehatan memberikan layanan sebaik mungkin. Tujuan digitalisasi kesehatan adalah untuk menyederhanakan dan mempermudah akses ke layanan kesehatan di Indonesia tanpa mengurangi kualitas dan efisiensi layanan tersebut. Digitalisasi kesehatan dapat menawarkan banyak manfaat seperti meningkatkan kualifikasi pelayanan kesehatan, mempermudah akses dan meningkatkan efisiensi dalam pelayanan kesehatan.

Untuk menunjang mutu pelaksanaan pelayanan kedokteran atau kesehatan yang berkualitas, rekam medik manual telah menjadi pedoman bagi pelayan kesehatan di Indonesia, sejak zaman belanda rekam medik sudah diterapkan dalam pencatatan tindakan yang diberikan kepada seorang pasien. Masalah yang seringkali muncul apabila sistem informasi rekam medis masih belum terintegrasi adalah tidak adanya keterkaitan antar masing-masing penyedia layanan kesehatan dalam hal informasi pada rekam medis. Menurut Kementerian Kesehatan melalui Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis, penerapan rekam medis elektronik dilakukan guna menjamin ketersediaan data yang akurat, lengkap, dan mudah diakses secara cepat oleh fasilitas pelayanan kesehatan. hadirnya UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi bertujuan untuk memberikan kerangka hukum yang efektif guna dapat diimplementasikan sehingga meminimalkan dampak yang berpotensi timbul akibat ancaman kebocoran data pribadi.

Pada dasarnya, setiap pasien mempunyai hak mendapatkan privasi dan kerahasiaan penyakit yang diderita termasuk data-data medisnya. privasi adalah hak yang dipunyai seseorang untuk menjaga kehidupan personal atau rahasia informasi personal agar hanya untuk diketahui sekelompok kecil saja. Sedikit berbeda dengan Cambridge Dictionary, Kamus Besar Bahasa Indonesia (KBBI) mendefinisikan privasi sebagai "kebebasan; keleluasaan pribadi." Senada dengan Pasal 28G ayat (1) Undang-Undang Dasar Tahun 1945, Pasal 2 huruf c UU

Adminduk menyatakan bahwa, Setiap Penduduk mempunyai hak untuk memperoleh perlindungan atas Data Pribadi. Hal ini secara tidak langsung menjadikan Negara memiliki kewajiban hukum sebagai pelindung pribadi setiap warga negaranya.

Di era digital saat ini, transformasi layanan kesehatan di Indonesia semakin masif, mulai dari penerapan Sistem Informasi Rumah Sakit hingga layanan telemedicine yang memudahkan pasien mengakses konsultasi medis secara daring. Namun, kemajuan ini sekaligus menghadirkan tantangan serius terkait perlindungan data pribadi pasien, yang meliputi informasi sensitif seperti riwayat kesehatan, identitas, dan lokasi pasien. Meskipun regulasi seperti UU Nomor 17 Tahun 2023 tentang Kesehatan dan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah memberikan kerangka hukum umum, perlindungan yang bersifat khusus dan teknis terhadap data medis masih belum memadai. Kondisi ini menimbulkan risiko kebocoran data, pelanggaran privasi, dan menurunnya kepercayaan publik terhadap sistem kesehatan digital.

N O	NAMA PENELITI AN	TAHU N	JUDUL PENELITIA N	PERSAMA AN	PERBEDAA N
1.	Lestari, A. Y., misras. DKK	2024	<i>Improving Healthcare Patient Data Security: An Integrated Framework Model for Electronic Health Records from a Legal Perspective.</i>	Penelitian kami sama- sama Menekankan pentingnya perlindungan data pasien dan hak pribadi; mengakui risiko kebocoran data.	Penelitian ini lebih bersifat teknis-solutif: menawarkan <i>framework</i> atau model integratif yang bisa diterapkan langsung oleh institusi kesehatan. Penelitian kami □ lebih bersifat normatif- advokatif: menekankan <i>urgensi</i> <i>pembentukan</i> <i>regulasi</i> <i>nasional</i> sebagai solusi kebijakan

					jangka panjang.
2.	Adi Herisasono	2024	<i>Perlindungan Hukum terhadap Privasi Data Pasien dalam Sistem Rekam Medis Elektronik</i>	Menekankan kepatuhan hukum, pengawasan, dan pendidikan SDM untuk melindungi data pasien.	Penelitian adi herisasono Lebih fokus pada aspek teknis dan operasional sistem rekam medis dan Penelitian kami fokus pada telemedicine, ancaman siber, dan pendekatan hukum progresif untuk keadilan pasien.
3.	Rospita Adelina Siregar & Haposan Sahala Raja Sinaga.	2025	<i>Aspek Hukum Perlindungan Data Pasien dalam Penyelenggaraan Rekam Medis Elektronik di Indonesia.</i>	Mengakui hak pasien atas kerahasiaan dan kontrol data pribadi; perlunya standar keamanan data.	Penelitian rospita Adelina DKK lebih fokus pada <i>rekam medis elektronik</i> sebagai bagian dari sistem informasi, dan membahas bagaimana regulasi yang ada mengatur teknis penyelenggaraan RME. Penelitian ini menyoroti urgensi pembentukan

					regulasi nasional khusus (lex specialis) untuk sektor kesehatan digital.
4.	WM Hendrata.	2025	<i>Legal Analysis of Patient Privacy Violation in Electronic Medical Records and Its Implications for Health Data Protection in Indonesia.</i>	Risiko digital dan penyalahgunaan data diakui; perlunya tata kelola dan kepatuhan.	Penelitian WM HENDRATA lebih bersifat <i>reaktif dan analitis</i> , menyoroti dampak dari pelanggaran yang sudah terjadi dan kelemahan hukum dalam menanganinya. a. Penelitian kami lebih bersifat <i>preventif dan kebijakan</i> , menyoroti perlunya regulasi baru sebelum terjadi pelanggaran.
5.	Hana Nur Hanifah & Arista Candra Irawati	2024	Urgensi Cyber Law dalam Menjaga Privasi Pasien di Rumah Sakit Era Digital	Sama-sama mengakui ancaman kebocoran data dan perlunya regulasi yang kuat.	Penelitian ini lebih menekankan pada aspek teknis dan ancaman dunia maya (cyber threats), serta pentingnya penerapan prinsip cyber

					law secara umum. Penelitian kami lebih menekankan pada urgensi pembentukan regulasi nasional yang sektoral dan spesifik untuk sistem informasi rumah sakit
--	--	--	--	--	--

Penelitian mengenai “Urgensi Pembentukan Regulasi Nasional Tentang Perlindungan Data Pasien Dalam Sistem Informasi Rumah Sakit” sangat penting dilakukan karena pembentukan regulasi ini sangat penting karena data pasien bersifat rentan dan menyangkut hak privasi yang dijamin konstitusi. Tanpa regulasi yang jelas, risiko kebocoran, penyalahgunaan, dan ketidakpastian hukum meningkat. Di era digital, rumah sakit wajib memiliki sistem informasi yang aman dan terintegrasi. Regulasi ini akan memberikan kepastian hukum bagi pasien sebagai pemilik data dan bagi rumah sakit sebagai pengendali data, sekaligus memperkuat kepercayaan publik terhadap layanan kesehatan digital.

Kasus kebocoran data pasien di aplikasi telemedicine di Indonesia menjadi salah satu peristiwa penting yang menggambarkan tantangan besar dalam pengelolaan keamanan data pribadi di era digital, khususnya dalam sektor kesehatan. Salah satu kasus yang menyita perhatian publik adalah kebocoran data pasien COVID-19 dan sistem e-HAC (Electronic Health Alert Card) yang terjadi pada tahun 2021. Insiden ini melibatkan bocornya data pribadi dalam jumlah besar yang berasal dari berbagai rumah sakit dan fasilitas kesehatan, dengan volume mencapai sekitar 720 GB.¹⁷ Data yang bocor tidak hanya berupa informasi umum seperti nama dan alamat pasien, tetapi juga mencakup data yang sangat sensitif seperti hasil tes COVID-19, foto rontgen, rekam medis, hingga dokumen administratif seperti surat rujukan BPJS dan surat persetujuan isolasi. Dalam kasus e-HAC, data dari lebih dari satu juta pengguna turut terekspos, termasuk informasi pribadi dan riwayat perjalanan yang seharusnya dijaga ketat kerahasiaannya.

Kebocoran data semacam ini sangat berisiko karena menyangkut hak privasi pasien atas informasi medisnya. Berdasarkan Pasal 58 ayat (1) dan (2) Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, setiap orang berhak atas kerahasiaan data dan informasi pribadi yang diberikan kepada tenaga kesehatan dan fasilitas pelayanan kesehatan. Bahkan dalam konteks perlindungan data pribadi secara umum, Pasal 2 dan Pasal 4 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dengan tegas menyebutkan bahwa

setiap pengendali data wajib menjamin keamanan data pribadi yang berada dalam penguasaannya, serta melindungi data dari akses, pengungkapan, dan penggunaan tanpa izin. Artinya, insiden ini jelas melanggar hak-hak fundamental pasien dan menyalahi kewajiban pengelola data.

Berdasarkan hasil penelitian, kebutuhan akan regulasi nasional yang secara khusus mengatur perlindungan data pasien dalam sistem informasi rumah sakit merupakan urgensi yang tidak dapat ditunda. Regulasi tersebut perlu berfungsi sebagai payung hukum terpadu yang mengharmoniskan prinsip perlindungan data, memperjelas kewenangan lembaga pengawas, menetapkan standar keamanan siber yang wajib dipenuhi rumah sakit, serta menegaskan kedudukan pasien sebagai pemilik data medisnya. Penyusunan regulasi yang komprehensif dan adaptif terhadap perkembangan teknologi dinilai memiliki peran strategis dalam memperkuat kepastian hukum, meningkatkan perlindungan hak pasien, serta membangun kepercayaan publik terhadap layanan kesehatan digital, sehingga tercipta perlindungan hukum yang lebih efektif dan berkeadilan bagi seluruh pemangku kepentingan.

Adapun yang menjadi rumusan masalah dalam penelitian ini untuk adalah untuk mengetahui: (1) Perlindungan Hak Pribadi dalam Implementasi Pengelolaan Data Pasien di Rumah Sakit (2) Urgensi Pembentukan Regulasi Nasional Khusus Yang Mengatur Perlindungan Data Pasien dan Konsep yang ideal untuk melindungi data pasien di era digitalisasi rumah sakit.

METODE

Penelitian ini menggunakan metode yuridis normatif yang dipadukan dengan pendekatan konseptual. Metode yuridis normatif digunakan untuk menelaah berbagai ketentuan hukum positif yang berkaitan dengan perlindungan data pribadi pasien, termasuk Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, Undang-Undang Rumah Sakit, serta berbagai peraturan teknis seperti Permenkes tentang rekam medis elektronik dan telemedicine. Melalui pendekatan normatif ini, penelitian mengidentifikasi kepastian hukum, keselarasan antaraturan, serta kelemahan-kelemahan normatif dalam pengaturan perlindungan data pasien di Indonesia. Sejalan dengan itu, penelitian ini menggunakan pendekatan konseptual untuk menelaah gagasan, asas, dan doktrin hukum yang mendasari perlindungan privasi dan kerahasiaan data kesehatan. Pendekatan ini mencakup analisis terhadap konsep hak privasi sebagai hak asasi manusia, kerahasiaan medis, hak kontrol pasien atas data, serta prinsip-prinsip perlindungan data internasional seperti lawfulness, fairness, transparency, purpose limitation, dan accountability. Pendekatan konseptual diperlukan karena isu perlindungan data pasien tidak hanya ditentukan oleh norma positif, tetapi juga oleh konstruksi teoritis yang membimbing penerapan hukum dalam konteks digital. Penggabungan pendekatan normatif dan konseptual memberikan kerangka analisis yang lebih komprehensif. Pendekatan normatif memungkinkan identifikasi kekosongan hukum, tumpang tindih regulasi, serta persoalan implementatif dalam sektor kesehatan digital. Sementara itu, pendekatan konseptual memungkinkan

perumusan landasan teoritis mengenai bagaimana regulasi perlindungan data seharusnya dirancang agar mampu menjawab tantangan digitalisasi sistem informasi rumah sakit. Melalui kedua pendekatan ini, penelitian dapat membangun argumentasi mengenai urgensi pembentukan regulasi nasional yang bersifat khusus, harmonis, dan adaptif terhadap perkembangan teknologi informasi dalam layanan kesehatan.

HASIL DAN PEMBAHASAN

Perlindungan Hak Pribadi dalam Implementasi Pengelolaan Data Pasien di Rumah Sakit

Perlindungan data pribadi adalah tanggung jawab yang ditetapkan dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang menyatakan bahwa: "setiap orang berhak mendapatkan perlindungan untuk diri pribadi, keluarga, kehormatan, martabat, serta harta benda yang berada di bawah kekuasaannya, dan juga berhak merasa aman serta dilindungi dari ancaman atau rasa takut untuk melakukan atau tidak melakukan sesuatu yang merupakan hak asasi manusia."

Di Indonesia telah diatur hak atas perlindungan diri pribadi, sebagaimana disebutkan dalam Pasal 28 G Ayat (1) bahwa warga negara berhak atas perlindungan diri pribadi, sebagai bagian dari Hak Asasi Manusia. Hak Pribadi ini bersifat sensitif karena terkait dengan data pribadi atau identitas seseorang yang terdapat dalam KTP (Kartu Tanda Penduduk), Paspor, SIM, Kartu Keluarga (KK), Nomor Pokok Wajib Pajak (NPWP), Nomor Rekeningbank serta Sidik jari. Dengan memberikan perlindungan terhadap hak pribadi tersebut, berarti juga memberikan perlindungan terhadap hak atas kebebasan berbicara yang menjamin perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi. Konsep perlindungan data pribadi ini menekankan bahwa setiap orang berhak untuk memutuskan ketika seseorang akan membagikan data kepada orang lain atau untuk berbagi data kepada orang lain serta menentukan kondisi yang harus dipenuhi selama proses berbagi data dalam sebuah komunitas.

Perlindungan data pribadi adalah landasan penting untuk mewujudkan sebuah masyarakat yang adil, aman, dan terjamin di era digital. Ini adalah kewajiban moral dan hukum yang harus diemban oleh semua pemangku kepentingan, dari perusahaan hingga individu, dalam upaya memastikan bahwa data pribadi dikelola dengan integritas dan kehati-hatian yang semestinya. UU PDP memberikan kerangka kerja yang komprehensif untuk mencapai tujuan ini dan menjadi dasar penting bagi perubahan budaya dan praktik terkait data pribadi. Kita harus menyadari bahwa dalam dunia yang semakin terkoneksi ini, perlindungan data pribadi adalah fondasi yang sangat penting untuk mencapai visi masyarakat yang cerdas, efisien, dan terjamin, yang memberikan manfaat seimbang antara teknologi dan privasi individu.

Menurut kami, meskipun perlindungan data pribadi penting di berbagai bidang, perlindungan data kesehatan membutuhkan perhatian yang jauh lebih besar terutama di rumah sakit. Data pasien bersifat sangat sensitif dan berpotensi

menimbulkan kerugian serius jika bocor. Dengan semakin banyaknya layanan kesehatan yang bergantung pada sistem digital, risiko kebocoran juga meningkat. Karena itu, menurut pandangan kami, perlindungan data pribadi secara umum belum cukup. Rumah sakit di Indonesia harus memiliki mekanisme khusus dan lebih ketat untuk menjaga keamanan data pasien agar kepercayaan masyarakat tetap terjaga.

Di Indonesia, tanggung jawab rumah sakit dalam menjaga privasi dan keamanan data pasien telah diatur melalui berbagai regulasi, meskipun belum terdapat preseden pengadilan yang secara langsung mengadili kasus kebocoran data rekam medis elektronik. Salah satu landasan hukum utama adalah Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, di mana Pasal 57 menegaskan bahwa informasi dalam rekam medis adalah milik pasien, sementara rumah sakit bertanggung jawab menjaga kerahasiaan dan integritas informasi tersebut. Dalam perkembangannya, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memberikan kerangka hukum yang lebih spesifik bagi seluruh penyelenggara sistem elektronik, termasuk rumah sakit, dalam menjamin perlindungan atas data pribadi pasien dari ancaman kebocoran, penyalahgunaan, atau akses ilegal.

Apabila ditinjau dari peraturan perundang-undangan, maka pada sektor kesehatan terdapat data pribadi yang wajib dilindungi baik itu data pribadi yang bersifat spesifik berupa data dan informasi kesehatan, data biometrik, dan data genetika, maupun data pribadi seperti nama, jenis kelamin, kewarganegaraan, agama, dan status perkawinan. Pada sektor kesehatan, pihak-pihak yang dapat dikategorikan sebagai Pengendali Data Pribadi adalah rumah sakit, penyelenggara layanan kesehatan serta perusahaan-perusahaan yang bergerak pada bidang medis lainnya. Di samping itu, pihak yang dapat dikategorikan sebagai pemrosesan data pribadi biasanya merupakan pihak ketiga dan/atau pihak lain yang ditunjuk oleh Pengendali Data Pribadi pada bidang kesehatan tersebut yang bertugas untuk melakukan pemrosesan data pribadi. Dengan demikian, pihak-pihak pada sektor kesehatan seperti rumah sakit, penyelenggara layanan kesehatan, dan lain-lain perlu tunduk pada UU PDP dan melaksanakan seluruh kewajiban yang melekat pada dirinya. Lebih lanjut, pihak-pihak yang terdapat pada sektor kesehatan seperti dokter, laboran, staff rumah sakit, dan pihak-pihak lainnya juga perlu tunduk pada UU PDP tersebut.

Bahwa di samping UU PDP, pengaturan khusus mengenai data pribadi pada sektor kesehatan juga diatur dalam Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan ("**UU Kesehatan**"). Adapun yang diatur adalah mengenai rahasia kesehatan, pengecualian terhadap kerahasiaan data kesehatan, dan rekam medis. Berdasarkan UU Kesehatan, setiap orang berhak untuk memperoleh kerahasiaan data dan informasi kesehatan pribadinya. Rahasia kesehatan sendiri meliputi data pribadi pasien yang merupakan data spesifik maupun data umum sebagaimana dikategorikan dalam UU PDP.

Bahwa apabila para pihak dalam sektor kesehatan tidak mengimplementasikan dan/atau tidak melaksanakan kewajiban sebagaimana telah diamanatkan oleh UU PDP, maka dapat dikenai sanksi yaitu berupa sanksi

administratif dan/atau sanksi pidana. Sanksi administratif sendiri dapat berupa; (i) peringatan tertulis; (ii) penghentian sementara kegiatan pemerosesan data pribadi; (iii) atau pemusnahan data pribadi; dan/atau (iv) denda administratif. Dalam hal adanya perbuatan melawan hukum dalam melakukan kewajiban perlindungan data pribadi, maka sanksi yang dapat diberikan adalah sanksi pidana sebagaimana diatur dalam Pasal 67 sampai dengan Pasal 72 UU PDP.

Meskipun regulasi tersebut memberikan perlindungan hukum yang kuat secara normatif, implementasinya masih menghadapi berbagai kendala, baik dalam aspek teknis, sumber daya manusia, maupun budaya hukum di institusi pelayanan kesehatan. Banyak rumah sakit lebih menitikberatkan pada pemenuhan administratif normatif, seperti sekadar menyusun SOP atau memasang sistem informasi, tanpa melakukan pengawasan, evaluasi, dan penguatan kapasitas secara menyeluruh. Pendekatan semacam ini dikritisi dalam paradigma hukum progresif yang menolak legalisme semata.

Urgensi Pembentukan Regulasi Nasional Khusus Yang Mengatur Perlindungan Data Pasien dan Konsep yang ideal untuk melindungi data pasien di era digitalisasi rumah sakit

Dalam era digital, keamanan data pribadi menjadi salah satu isu penting yang perlu mendapat perhatian serius, terutama pada sektor publik yang mengelola informasi sensitif masyarakat. Pentingnya perlindungan data pribadi, khususnya dalam bidang kesehatan, semakin mendalam dengan meningkatnya penggunaan teknologi dalam pengelolaan data. Perlindungan data pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia saat ini belum berjalan maksimal, hal ini ditunjukkan dengan masih banyaknya pelanggaran terhadap penyalahgunaan data pribadi akibat dari semakin berkembangnya penggunaan digital platform yang tidak disertai dengan perlindungan hukum yang memadai.

Namun demikian, perkembangan teknologi informasi saat ini dapat dianggap sebagai sebuah pedang bermata dua karena dapat memberikan manfaat dan peningkatan kesejahteraan, sekaligus sarana dalam melakukan kejahatan. Kejahatan-kejahatan yang timbul pada bidang data pribadi di Indonesia biasa dilakukan dengan menggunakan jaringan internet, seperti penipuan, hacking, penyadapan data orang lain, spamming email, dan manipulasi data untuk mengakses data milik orang lain. Kemajuan teknologi informasi telah mengakibatkan batas privasi semakin berkurang, sehingga berbagai data pribadi semakin mudah tersebar dan/atau didapatkan oleh orang-orang yang tidak bertanggung jawab. Padahal, Data pribadi adalah suatu hal yang melekat pada diri setiap orang tanpa terkecuali, dimana data pribadi merupakan hal yang wajib dilindungi dan tergolong kedalam hak privasi seseorang. Hak privasi di Indonesia adalah hak konstitusional warga negara yang telah diatur di dalam Undang-Undang Dasar Republik Indonesia Tahun 1945.

Bawasannya Indonesia sebagai negara hukum telah berusaha untuk mengatasi permasalahan yang berkaitan dengan data pribadi tersebut dengan menciptakan dan/atau mengesahkan Undang-Undang Nomor 27 Tahun 2022

tentang Perlindungan Data Pribadi (“UU PDP”). Adapun UU PDP telah mengatur mengenai asas, jenis data pribadi, hak subjek data pribadi, pemerosesan data pribadi, larangan dalam penggunaan data pribadi, dan beberapa hal terkait data pribadi lainnya. Berkaitan dengan bidang kesehatan, UU PDP mengatur mengenai data pribadi yang spesifik seperti informasi kesehatan, data biometrik, data genetika, catatan kesehatan, dan data lainnya. Hal ini menunjukkan bahwa UU PDP juga mengatur dan memperhatikan mengenai pentingnya privasi dalam pengelolaan data pada bidang kesehatan, namun demikian implementasi terhadap perlindungan data pribadi tersebut belum banyak diterapkan dan/atau dipersiapkan, mengingat UU PDP memberikan waktu selama 2 (dua) tahun untuk dilakukan penyesuaian. Lebih lanjut, lahirnya UU PDP menimbulkan berbagai tantangan pada bidang kesehatan, termasuk namun tidak terbatas pada penyesuaian peraturan dan praktik kesehatan, penyesuaian dengan etika medis, dan berbagai macam hal lainnya. Secara khusus penulisan ini diharapkan dapat menjadi rujukan dalam pelaksanaan implementasi perlindungan data pribadi di sektor kesehatan. Selain itu, penulisan ini diharapkan juga dapat memberikan informasi mengenai tantangan-tantangan yang akan timbul terkait dengan perlindungan data pribadi pada bidang kesehatan, sehingga para praktisi pada bidang sektor kesehatan dapat mempersiapkan diri dalam menghadapi berbagai tantangan dimaksud

Dalam implementasinya, masalah utama terjadi pada aspek penegakan hukum dan keterbatasan pengawasan. Meskipun UU PDP memiliki pasal-pasal yang memuat ketentuan sanksi administratif maupun pidana atas pelanggaran terhadap data pribadi, mekanisme monitoring dan penegakannya masih menghadapi tantangan, khususnya dalam lingkungan digital yang dinamis dan melibatkan banyak pihak lintas batas yurisdiksi. Selain itu, tantangan lain yang tidak kalah serius adalah resistensi dari penyelenggara layanan kesehatan yang masih menganggap regulasi perlindungan data sebagai beban administratif semata. Kurangnya investasi pada sistem keamanan siber dan minimnya pelatihan keamanan data di fasilitas kesehatan menimbulkan risiko berkelanjutan dalam praktik telemedicine. Kedisiplinan penyedia layanan dalam mengantongi informed consent dari pasien patut mendapat perhatian khusus. Banyak aplikasi telemedicine masih menggunakan format persetujuan yang tidak jelas, atau menggabungkan persetujuan penggunaan data dengan syarat dan ketentuan layanan, sehingga tidak benar-benar memenuhi prinsip transparansi dan kebebasan memilih dari pasien.

Melihat kompleksitas persoalan tersebut, jelas bahwa isu perlindungan data tidak hanya berhenti pada fasilitas kesehatan. Justru tantangan terbesar muncul pada lembaga publik yang mengelola data kesehatan dalam skala masif. Di sinilah penting untuk melihat bagaimana standar perlindungan data diterapkan pada BPJS Kesehatan, karena setiap celah keamanan pada level ini akan berdampak jauh lebih besar bagi jutaan peserta JKN. Dengan kata lain, sebelum bicara implementasi teknis, terlebih dahulu harus dipastikan bahwa lembaga negara yang memegang otoritas data sensitif benar-benar memenuhi tanggung jawab hukumnya.

Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan merupakan badan hukum publik yang dibentuk berdasarkan Undang-Undang Nomor 24 Tahun 2011.

Sebagai lembaga negarayang bertanggung jawab menyelenggarakan program Jaminan Kesehatan Nasional (JKN), BPJS Kesehatan memiliki akses terhadap data pribadi peserta yang sangat sensitif, termasuk informasi identitas, riwayat penyakit, rekam medis, hingga data sosial dan ekonomi. Data tersebut bukan hanya menjadi instrumen teknis penyelenggaraan layanan, melainkan jugamerupakan hak privat yang harus dilindungi secara ketat sesuai dengan prinsip hukum dan etika. Dalam konteks hukum, pengelolaan data peserta JKN bukan semata-mata kewenangan administratif, melainkan juga merupakan tanggung jawab hukum yang melekat pada BPJS Kesehatan sebagai badan publik. Data yang dikumpulkan, disimpan, dan digunakan oleh BPJS tidak dapat diperlakukan sebagai informasi terbuka, karena mengandung unsur kerahasiaan dan potensi dampak signifikan terhadap hak-hak peserta jika disalahgunakan atau dibocorkan.

Teori tanggung jawab hukum menjadi pendekatan yang tepat dalam menganalisis kewajiban BPJS Kesehatan atas perlindungan dan pengelolaan data peserta. Menurut teori ini, setiap pelaku hukum (termasuk badan publik) yang melanggar ketentuan hukum dan menimbulkan kerugian bagi pihak lain, harus bertanggung jawab secara hukum baik secara administratif, perdata, maupun pidana. Dalam hal ini, BPJS wajib bertanggung jawab apabila terjadi penyalahgunaan, kebocoran, atau kelalaian dalam pengelolaan data pribadi peserta. Tanggung jawab hukum BPJS juga berakar dari asas legalitas yang mengharuskan setiap tindakan lembaga publik didasarkan pada hukum. UU Nomor 24 Tahun 2011 secara eksplisit menyatakan bahwa BPJS harus menjaga dan melindungi kerahasiaan data peserta. Ketentuan ini diperkuat oleh UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP), yang mengklasifikasikan data kesehatan sebagai data pribadi sensitif dan mewajibkan pengendali data, seperti BPJS, untuk memastikan kerahasiaan, integritas, dan akuntabilitas dalam pengelolaan data. Tanggung jawab hukum BPJS juga bisa ditinjau dari segi tanggung jawab administratif.

Namun, meskipun BPJS Kesehatan memiliki kewajiban hukum yang jelas, persoalan perlindungan data tidak berhenti pada norma tertulis. Justru celah pada pengawasan dan lemahnya penegakan membuat isu kebocoran data terus berulang. Kondisi ini memperlihatkan bahwa tanggung jawab kelembagaan saja tidak cukup, sehingga diperlukan pembahasan lebih lanjut mengenai problem sanksi, transparansi, dan kebutuhan regulasi nasional yang benar-benar mampu melindungi data pasien secara efektif.

Di sisi lain, kurangnya sanksi tegas serta masih lemahnya pengawasan dari otoritas berwenang menyebabkan pelanggaran privasi kerap kali tidak ditindaklanjuti secara efektif. Meski UU PDP mewajibkan pelaporan insiden pelanggaran data pribadi, dalam praktiknya mekanisme ini jarang diimplementasikan secara terbuka oleh penyedia layanan, dan seringkali publik baru mengetahui adanya kebocoran data setelah kasus menjadi viral di media). Beberapa upaya telah dilakukan untuk meningkatkan kapasitas perlindungan data pasien, termasuk program sosialisasi, pelatihan keamanan digital, serta peningkatan standar infrastruktur dan teknologi pada layanan telemedicine. Pemerintah juga mendorong kolaborasi lintas sektor antara regulator, penyedia

layanan, dan masyarakat guna memperkuat akuntabilitas dan membangun ekosistem keamanan data yang lebih transparan.

Penegakan prinsip-prinsip perlindungan data internasional seperti lawfulness, fairness, dan transparency juga perlu dipertegas dalam pedoman teknis sektor kesehatan digital. Hal ini penting untuk membangun kepercayaan masyarakat, mengingat sensitivitas data medis sangat tinggi dan sering menjadi target serangan siber maupun penyalahgunaan oleh pihak tidak bertanggung jawab. Dengan demikian, pembentukan regulasi nasional khusus menjadi kebutuhan mendesak untuk menjamin hamid kepastian hukum, meningkatkan kepercayaan publik, serta mewujudkan tata kelola data pasien yang aman, transparan, dan sesuai dengan prinsip hak asasi manusia di era digital.

Melihat lemahnya pengawasan, ketidakkonsistenan penegakan, dan masih terbukanya celah kebocoran data bahkan pada lembaga besar seperti BPJS Kesehatan, semakin tampak bahwa kerangka hukum yang ada belum mampu mengimbangi kompleksitas pengelolaan data kesehatan di era digital. Aturan saat ini tidak cukup rinci, tidak operasional, dan belum memberi jaminan perlindungan yang kuat bagi pasien. Karena itu, kebutuhan akan regulasi nasional yang khusus dan lebih tegas bukan lagi sekadar wacana, tetapi tuntutan nyata agar hak privasi pasien terlindungi dan tata kelola data di rumah sakit dapat berlangsung secara aman dan akuntabel.

Pengaturan hak dan kewajiban pasien dalam sistem hukum kesehatan Indonesia kini diatur oleh Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, yang menegaskan hak pasien atas pelayanan berkualitas, informasi medis yang jelas, dan persetujuan tindakan medis berbasis informasi. Namun, dalam implementasinya, masih ditemukan kendala seperti ketimpangan informasi antara tenaga medis dan pasien yang dapat melemahkan perlindungan hak pasien. Pengaturan kewajiban pasien untuk memberikan informasi akurat dan mematuhi prosedur medis menunjukkan pentingnya tanggung jawab bersama dalam proses pengobatan. Peneliti menilai bahwa selain kerangka hukum yang memadai, edukasi hukum bagi pasien, pengawasan, dan penerapan praktik pelayanan yang etis menjadi kunci agar hak pasien terlindungi secara nyata di lapangan.

Untuk itu, diperlukan upaya perbaikan dalam beberapa aspek, seperti peningkatan edukasi dan sosialisasi tentang hak dan kewajiban pasien kepada masyarakat dan tenaga medis, penguatan pengawasan terhadap fasilitas kesehatan dan praktik medis, serta perbaikan aksesibilitas dan kualitas pelayanan kesehatan di seluruh wilayah Indonesia. Dengan langkah-langkah tersebut, diharapkan sistem hukum kesehatan Indonesia dapat lebih efektif dalam melindungi hak-hak pasien dan memastikan tercapainya keseimbangan yang adil antara hak pasien dan kewajiban yang harus dilaksanakan oleh pasien dan tenaga medis.

Walaupun peraturan secara normatif telah ada, kenyataan di lapangan menunjukkan bahwa pelaksanaan perlindungan data masih belum berjalan secara efektif. Hal ini disebabkan oleh banyak faktor, termasuk aspek teknis, regulasi, keterbatasan sumber daya manusia, dan juga ancaman eksternal yang semakin rumit di zaman digital. Berbagai tantangan yang dihadapi:

a. Keterbatasan Infrastruktur Teknologi Informasi

Banyak rumah sakit, terutama yang berada di wilayah terpencil, masih menghadapi masalah dengan infrastruktur teknologi informasi. Penggunaan sistem informasi manajemen rumah sakit yang tidak sesuai standar dan tidak dilindungi dengan enkripsi dapat meningkatkan risiko kebocoran data. Bahkan, banyak dari rumah sakit tersebut belum memiliki sistem untuk mencadangkan data atau sistem keamanan siber seperti firewall, antivirus, dan cara untuk mendeteksi intrusi.

Berdasarkan informasi dari Kementerian Kesehatan, hanya sekitar 40% rumah sakit yang sudah memiliki Sistem Informasi Manajemen Rumah Sakit yang terintegrasi serta aman secara digital. Ini menunjukkan bahwa kesiapan teknologi masih lemah untuk memenuhi persyaratan regulasi, seperti yang diatur dalam Permenkes No. 24 Tahun 2022 dan UU PDP yang mengharuskan keamanan data pasien secara elektronik.

b. Rendahnya Pemahaman dan Kesadaran SDM

kesehatan, administrator, dan manajemen rumah sakit sering kali tidak memiliki pemahaman yang mendalam tentang aturan perlindungan data pribadi dan etika privasi pasien. Pemahaman mengenai betapa pentingnya menjaga kerahasiaan data pasien masih belum merata, sehingga tindakan seperti mengakses data tanpa izin, mengirim data melalui saluran yang tidak aman (misalnya aplikasi pesan instan), atau menyimpan data di perangkat pribadi masih sering terjadi.

Kelemahan ini dapat menyebabkan risiko pelanggaran hukum, baik secara sengaja maupun akibat kelalaian. Namun, sesuai dengan UU PDP, pengendali data wajib memastikan bahwa hanya pihak yang berwenang yang dapat mengakses dan memproses data pribadi pasien.

c. Ancaman Serangan Siber

Serangan siber yang menargetkan institusi layanan kesehatan telah mengalami peningkatan yang signifikan di tingkat global dan nasional. Informasi dari Kementerian Komunikasi dan Informatika menunjukkan bahwa sektor kesehatan menjadi salah satu sasaran utama untuk peretasan data pada tahun 2022 hingga 2023. Rumah sakit, sebagai penyedia layanan publik, sangat rentan karena data yang mereka simpan sangat berharga, seperti riwayat medis, informasi identitas, dan data keuangan pasien.

Ancaman yang berupa ransomware, phishing, serta pelanggaran data tidak hanya merugikan institusi dari segi reputasi dan keuangan, tetapi juga berdampak langsung pada hak pasien terhadap privasi dan kerahasiaan informasi.

d. Ketidaksinkronan Regulasi

Satu tantangan lainnya adalah adanya tumpang tindih dan ketidaksesuaian antara regulasi teknis di setiap sektor seperti Permenkes No. 24/2022, UU Kesehatan, serta UU PDP. Beberapa aturan teknis masih perlu diperbarui agar selaras dengan prinsip-prinsip yang terdapat dalam UU PDP, seperti penunjukan Data Protection Officer (DPO), kewajiban melakukan penilaian dampak privasi, serta pelaporan insiden yang berkaitan dengan pelanggaran data.

Di samping itu, tidak semua rumah sakit menyadari atau memahami sanksi administratif dan pidana yang berlaku jika terjadi pelanggaran. Keadaan ini menyebabkan kurangnya urgensi untuk membangun struktur perlindungan data yang kokoh dan berkelanjutan.

Untuk menjawab berbagai tantangan di atas, diperlukan langkah-langkah konkret yang bersifat sistemik, kolaboratif, dan progresif. Upaya tersebut antara lain:

a. Penguatan Infrastruktur dan Keamanan Siber

Menurut kami, penguatan infrastruktur dan keamanan siber di rumah sakit bukan sekadar kebutuhan teknis, tetapi menjadi bagian krusial dalam melindungi data pribadi pasien di era digital. Investasi pada sistem TI yang andal, mulai dari perangkat keras, perangkat lunak, hingga sumber daya manusia di bidang TI, harus menjadi prioritas agar data medis dapat disimpan dan dikelola secara aman. Implementasi sistem rekam medis elektronik sebaiknya dilengkapi dengan enkripsi, autentikasi ganda, serta sistem pencadangan dan pemulihan bencana digital. Selain itu, keterlibatan profesional keamanan siber untuk melakukan audit dan pemantauan sistem secara berkala menjadi langkah penting untuk mencegah kebocoran atau penyalahgunaan data. Menurut saya, langkah-langkah tersebut tidak hanya memenuhi amanat Pasal 39 UU PDP terkait prinsip *privacy by design* dan *security by default*, tetapi juga menunjukkan komitmen nyata rumah sakit dalam membangun kepercayaan pasien terhadap keamanan data pribadi mereka.

b. Pendidikan dan Pelatihan SDM

Pengembangan kemampuan sumber daya manusia sangat krusial untuk melaksanakan peraturan. Rumah sakit harus mengadakan pelatihan secara teratur untuk staf medis, pekerja administrasi, dan tim TI tentang dasar-dasar perlindungan data pribadi, etika dalam bidang medis, serta pengolahan data sesuai dengan undang-undang yang berlaku.

Pelatihan ini mencakup tidak hanya aspek teknis, tetapi juga elemen etika dan hukum agar setiap anggota tim memahami pentingnya pengamanan data pasien. Pendidikan serta pelatihan untuk sumber daya manusia menjadi hal yang krusial dalam mendukung keberhasilan penerapan peraturan mengenai perlindungan data pribadi pasien. Para tenaga kesehatan, pegawai administrasi, dan petugas teknologi informasi di rumah sakit perlu dibekali dengan pengetahuan menyeluruh tentang prinsip privasi dasar, regulasi yang berlaku termasuk Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta etika dalam pengelolaan informasi medis. Pelatihan ini seharusnya berjalan terus-menerus dan dapat beradaptasi dengan perkembangan teknologi, termasuk simulasi risiko siber, prosedur pelaporan insiden kebocoran data, dan langkah-langkah menangani akses yang tidak sah. Dengan menciptakan budaya yang menyadari pentingnya privasi dan meningkatkan keterampilan sumber daya manusia, rumah sakit bisa mengurangi kemungkinan pelanggaran hukum sekaligus menjaga keyakinan pasien terhadap sistem pelayanan kesehatan digital.

c. Penunjukan Data Protection Officer (DPO)

UU PDP mengatur bahwa setiap pengendali data pribadi yang melakukan pemrosesan data dalam skala besar atau sensitif wajib menunjuk Data Protection Officer (DPO). Dalam konteks rumah sakit, DPO bertugas untuk memastikan kepatuhan terhadap UU PDP, mengawasi pengelolaan data, serta menjadi penghubung antara rumah sakit dengan otoritas pengawas. Dengan adanya DPO,

rumah sakit akan memiliki pengawasan internal yang lebih efektif dan struktur manajemen risiko yang lebih baik terhadap pelanggaran data pribadi.

Penunjukan DPO merupakan langkah strategis yang wajib dilakukan oleh rumah sakit sebagai bentuk kepatuhan terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. DPO bertanggung jawab atas pengawasan kepatuhan terhadap pengelolaan data pribadi, termasuk merancang kebijakan perlindungan data, melakukan audit internal, memberikan rekomendasi atas potensi risiko, serta menjadi penghubung antara rumah sakit dan otoritas perlindungan data. Dalam konteks rumah sakit, DPO juga berperan penting dalam memastikan bahwa data pasien, terutama rekam medis elektronik, dikelola dengan prinsip kehati-hatian dan tidak disalahgunakan oleh pihak yang tidak berwenang.

Oleh karena itu, pemilihan DPO harus mempertimbangkan kompetensi teknis dan pemahaman hukum yang memadai agar peran ini dapat dijalankan secara profesional dan efektif dalam mendukung tata kelola data pribadi yang aman di era digital.

d. Penyusunan SOP dan Audit Berkala

Rumah sakit perlu menyusun dan menetapkan standar operasional prosedur (SOP) terkait perlindungan data pribadi, mulai dari proses pengumpulan data, penyimpanan, pemanfaatan, hingga penghapusan data. SOP tersebut harus disesuaikan dengan prinsip-prinsip perlindungan data dalam UU PDP dan regulasi sektoral. Audit berkala perlu dilakukan, baik secara internal maupun oleh pihak ketiga, untuk mengukur kepatuhan dan mengevaluasi potensi kelemahan sistem.

Penyusunan Standar Operasional Prosedur (SOP) dan audit berkala merupakan instrumen penting dalam menjamin konsistensi dan kepatuhan rumah sakit terhadap regulasi perlindungan data pribadi. SOP harus mencakup seluruh proses pengelolaan data, mulai dari pengumpulan, penyimpanan, penggunaan, hingga pemusnahan data, dengan memperhatikan prinsip transparansi, minimalisasi data, serta keamanan. Prosedur ini wajib disosialisasikan kepada seluruh unit kerja agar menjadi pedoman yang mengikat dan operasional. Selain itu, audit internal maupun eksternal perlu dilakukan secara berkala untuk mengevaluasi efektivitas pelaksanaan SOP, mendeteksi potensi pelanggaran, dan memberikan rekomendasi perbaikan. Dengan adanya SOP yang jelas dan audit yang rutin, rumah sakit dapat meningkatkan akuntabilitas serta mencegah terjadinya kebocoran atau penyalahgunaan data pribadi pasien secara sistematis.

Meskipun Indonesia telah memiliki landasan hukum yang kuat melalui UU PDP dan regulasi sektoral lainnya, implementasi di lapangan masih menghadapi berbagai tantangan serius. Rumah sakit sebagai institusi vital harus melakukan transformasi internal secara menyeluruh, mulai dari peningkatan infrastruktur hingga penguatan tata kelola data. Perlindungan data pribadi pasien bukan hanya soal teknis, tetapi menyangkut hak asasi manusia dan kepercayaan publik terhadap layanan kesehatan. Ke depan, kolaborasi antara pemerintah, rumah sakit, organisasi profesi, dan masyarakat menjadi kunci untuk menciptakan ekosistem kesehatan digital yang aman, adil, dan akuntabel.

SIMPULAN

Kesimpulan dari penelitian ini menegaskan bahwa perlindungan data pribadi pasien dalam sistem informasi rumah sakit merupakan kewajiban hukum, moral, dan konstitusional yang harus diwujudkan secara nyata dalam praktik pelayanan kesehatan di era digital. Meskipun Indonesia telah memiliki sejumlah regulasi seperti UU Kesehatan dan UU Perlindungan Data Pribadi, implementasinya masih menghadapi berbagai kendala, mulai dari ketidaksinkronan aturan, lemahnya infrastruktur dan keamanan siber, rendahnya literasi digital serta kesadaran tenaga kesehatan, hingga tantangan penegakan hukum. Kondisi tersebut menunjukkan bahwa perlindungan yang ada masih bersifat sektoral dan belum memberikan jaminan menyeluruh terhadap hak privasi pasien. Oleh karena itu, diperlukan pembentukan regulasi nasional khusus yang bersifat integratif, operasional, dan tegas, yang mampu mengatur standar keamanan siber, tata kelola data pasien, kewajiban serta tanggung jawab hukum pihak terkait, dan mekanisme pengawasan yang efektif, sehingga tercipta perlindungan hukum yang komprehensif, kepastian hukum yang kuat, serta meningkatnya kepercayaan publik terhadap layanan kesehatan digital di Indonesia.

DAFTAR RUJUKAN

- Adi Sutrisno, and Arief Budiono. "Perlindungan Hukum Dalam Kualitas Pelayanan Medis Terhadap Hak Dan Privasi Pasien Rawat Inap (Studi Kasus Di Rumah Sakit Umum Daerah Provinsi Papua Barat)." *Sehat Rakyat: Jurnal Kesehatan Masyarakat* 4, no. 2 (2025): 311–29.
<https://doi.org/10.54259/selhatrakyat.v4i2.4346>.
- Al-irfani, Adib Wajih, and Hudi Yusuf. "HUKUM KESEHATAN INDONESIA SETTING OF PATIENT RIGHTS AND OBLIGATIONS IN THE INDONESIAN," 2025, 1420–21.
- Disemadi, Hari Sutra, Lu Sudirman, Junimart Girsang, and Meida Aninda. "Perlindungan Data Pribadi Di Era Digital : Mengapa Kita Perlu Peduli ?" 1, no. 2 (2023): 81.
- Hak, Perlindungan, and Asasi Manusia. "Rosihan Luthfi" 2, no. 5 (2022): 433.
- Hukum, Fakultas, and Universitas Tarumanagara. "Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.5. No.12 (2024) Tema/ELdisi : Hukum Dan Hak Asasi Manusia (Bulan Kedua Belas) <https://Jhlg.Rewangrencang.Com/>" 5, no. 12 (2024): 7.
- Jurnal, Hakim, and Ilmu Hukum. "Kewajiban Dan Tanggung Jawab Hukum Perdata Dalam Perlindungan Privasi Data Pasien Dalam Layanan Kesehatan Digital Mohamad Rizky Ardiansyah" 3, no. 4 (2023).
- Maria, Indah, Maddalena Simamora, Fakultas Hukum, and Universitas Taumanagara. "PERLINDUNGAN HUKUM ATAS HAK PRIVASI DAN KERAHASIAAN IDENTITAS PENYAKIT BAGI PASIEN COVID-19" 1, no. 7 (2009): 1091.
- Mau, Hedwig, Tinggi Hukum Militer, Article Info, and Article History. "Tanggungjawab Hukum Badan Penyelenggara Jaminan Sosial Kesehatan Dalam Pengelolaan Dan Perlindungan Data Peserta Jaminan Kesehatan

- Tehadap Risiko Kebocoran Data” 8 (2025): 12077.
- Memo, Lukito, and Gani Ascobat. “PELAYANAN KESEHATAN YANG EFISIEN DAN TERJANGKAU MELALUI TRANSFORMASI K\SEHATAN DIGITAL VIA TELLEMEDICINE DI INDONESIA” XIV, no. 2 (n.d.): 109.
- Mubarak, Haikal, mas Rosidawati Wiradirja, and Nugraha Pranadita. “Penegakan Hukum Terhadap Tanggungjawab Rumah Sakit Pada Pengelolaan Privasi Dan Keamanan Rekam Medis Elektronik Dalam Perspektif Hukum Progrelsif Di Indonesia” 6, no. 2 (2025): 72.
- Nadiroh, Aenun, and Sidi Ahyar Wiraguna. “Analisis Yuridis Kebocoran Data Di Layanan Kesehatan Digital: Studi Kasus Aplikasi Tellementicine Di Indonesia” 2, no. 6 (2025): 248.
- Sorisa, Cinda, and Cindi Lusua Kiareni. “Etika Keamanan Siber : Studi Kasus Kebocoran Data BPJS Kesehatan Di Indonesia” 2, no. 6 (2024): 586.
- Widjaja, Gunawan, Dyah Ersita Yustanti, Hotmaria Hertawaty Sijabat, Handojo Dhanudibroto, and Doctoral Student. “IMPLEMENTASI PERLINDUNGAN DATA PRIBADI PASIEN DALAM LAYANAN TELLELMEDICINE DI INDONESIA : ANALISIS REGULASI DAN” 3, no. 2 (2025): 153.
- Yuridis, Tinjauan, Perlindungan Data, and Pribadi Pada. “SYNERGY Jurnal Ilmiah Multidisiplin” 1, no. 4 (2024): 250–51.