



PRINSIP HUKUM KEPAILITAN DI INDONESIA

Ardian Harefa

Guru Nias Selatan

Email : ardianharefa20@gmail.com

Abstrak

Transformasi digital dalam pelayanan kesehatan melalui penerapan rekam medis elektronik dan sistem informasi rumah sakit telah meningkatkan efisiensi, efektivitas, dan kualitas pelayanan kesehatan. Namun, digitalisasi tersebut juga menimbulkan risiko yang semakin besar terhadap pelanggaran privasi pasien akibat kebocoran, penyalahgunaan, atau akses tanpa hak terhadap data kesehatan yang bersifat sensitif. Penelitian ini bertujuan untuk menganalisis perlindungan hukum terhadap privasi pasien serta pertanggungjawaban hukum rumah sakit sebagai badan hukum apabila terjadi kebocoran data elektronik pasien. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier yang dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa data kesehatan merupakan data pribadi spesifik yang memperoleh perlindungan khusus berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, serta peraturan mengenai rekam medis elektronik. Rumah sakit sebagai pengendali data memiliki kewajiban hukum untuk menjamin keamanan, kerahasiaan, integritas, dan ketersediaan data pasien melalui penerapan tata kelola keamanan informasi yang memadai. Apabila terjadi kebocoran data akibat kelalaian rumah sakit, maka rumah sakit dapat dimintai pertanggungjawaban secara administratif, perdata, maupun pidana sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. Oleh karena itu, diperlukan penguatan tata kelola perlindungan data pribadi, peningkatan standar keamanan sistem elektronik, serta pengawasan yang lebih efektif guna menjamin perlindungan hak privasi pasien dalam penyelenggaraan pelayanan kesehatan digital.

Kata Kunci: Privasi Pasien; Pelindungan Data Pribadi; Rekam Medis Elektronik; Rumah Sakit; Kebocoran Data; Pertanggungjawaban Hukum.

Abstract

The digital transformation of healthcare services through the implementation of electronic medical records and hospital information systems has significantly improved the efficiency, effectiveness, and quality of healthcare delivery. However, this transformation has also increased the risk of patient privacy violations arising from data breaches, unauthorized access, and misuse of sensitive health information. This study aims to analyze the legal protection of patient privacy and the legal liability of hospitals as legal entities in the event of electronic patient data breaches. The research employs a normative legal research method using statutory and conceptual approaches. The legal materials consist of primary, secondary, and tertiary legal sources, which are analyzed qualitatively. The findings indicate that health data constitute a category of sensitive personal data that receives special protection under Law Number 27 of 2022 on Personal Data Protection, Law Number 17 of 2023 on Health, and regulations governing electronic medical records. As data controllers, hospitals are legally obligated to ensure the confidentiality, integrity, availability, and security of patients' personal data by implementing effective information security governance. Where a data breach results from the negligence or failure of a hospital to fulfill its legal obligations, the hospital may incur administrative, civil, and criminal liability in accordance with the applicable laws and



regulations. Therefore, strengthening personal data governance, enhancing electronic information security standards, and improving regulatory oversight are essential to ensuring effective protection of patient privacy within Indonesia's digital healthcare system.

Keywords: *Patient Privacy; Personal Data Protection; Electronic Medical Records; Hospitals; Data Breach; Legal Liability.*

I. PENDAHULUAN

A. Latar Belakang

Transformasi digital dalam sektor kesehatan telah mengubah paradigma penyelenggaraan pelayanan kesehatan di berbagai negara, termasuk Indonesia. Digitalisasi pelayanan kesehatan melalui penerapan rekam medis elektronik (electronic medical records), sistem informasi rumah sakit, layanan telemedicine, dan integrasi data kesehatan nasional memberikan berbagai manfaat, seperti peningkatan efisiensi pelayanan, percepatan pengambilan keputusan klinis, kemudahan koordinasi antar tenaga kesehatan, serta peningkatan kualitas pelayanan kepada masyarakat. Namun demikian, di balik berbagai manfaat tersebut, digitalisasi juga menghadirkan tantangan baru berupa meningkatnya risiko pelanggaran privasi pasien akibat kebocoran, penyalahgunaan, maupun akses tanpa hak terhadap data kesehatan yang tersimpan dalam sistem elektronik. Data kesehatan merupakan salah satu kategori data pribadi yang paling sensitif karena memuat informasi mengenai kondisi fisik, mental, riwayat penyakit, diagnosis, tindakan medis, hingga informasi genetik seseorang. Oleh karena itu, perlindungan terhadap data kesehatan menjadi bagian yang tidak terpisahkan dari perlindungan hak asasi manusia, khususnya hak atas privasi.

Hak atas privasi pasien merupakan hak fundamental yang melekat pada setiap individu dalam memperoleh pelayanan kesehatan. Hubungan antara pasien dengan rumah sakit dibangun atas dasar kepercayaan (fiduciary relationship), sehingga pasien bersedia memberikan berbagai informasi yang bersifat sangat pribadi dengan keyakinan bahwa seluruh

informasi tersebut akan dijaga kerahasiaannya dan hanya digunakan untuk kepentingan pelayanan kesehatan. Apabila rumah sakit gagal menjaga kerahasiaan tersebut, maka kerugian yang dialami pasien tidak hanya berupa kerugian ekonomi, tetapi juga dapat berupa kerugian sosial, psikologis, maupun hilangnya kepercayaan masyarakat terhadap sistem pelayanan kesehatan. Dengan demikian, perlindungan privasi pasien bukan sekadar kewajiban etik profesi kesehatan, melainkan juga merupakan kewajiban hukum yang harus dipenuhi oleh rumah sakit sebagai penyelenggara pelayanan kesehatan sekaligus sebagai pengendali data pribadi.

Urgensi perlindungan privasi pasien semakin meningkat seiring berkembangnya penggunaan rekam medis elektronik. Berbeda dengan rekam medis konvensional, data elektronik dapat diproses, dipindahkan, disalin, maupun diakses dalam jumlah besar melalui jaringan elektronik sehingga memiliki tingkat kerentanan yang jauh lebih tinggi terhadap berbagai ancaman keamanan siber, seperti hacking, ransomware, phishing, penyalahgunaan hak akses oleh pegawai internal, maupun kegagalan sistem keamanan informasi. Berbagai insiden kebocoran data rumah sakit yang terjadi di berbagai negara menunjukkan bahwa data kesehatan memiliki nilai ekonomi yang tinggi dan menjadi salah satu target utama kejahatan siber. Kebocoran data tersebut berpotensi menyebabkan pencurian identitas, penipuan, diskriminasi, pemerasan, hingga penyalahgunaan informasi medis yang dapat merugikan pasien dalam jangka panjang.



Di Indonesia, perlindungan terhadap data kesehatan memperoleh dasar hukum melalui berbagai peraturan perundang-undangan, antara lain Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Peraturan Menteri Kesehatan mengenai Rekam Medis Elektronik, serta berbagai ketentuan lain yang mengatur penyelenggaraan sistem elektronik. Regulasi tersebut menempatkan data kesehatan sebagai data pribadi spesifik yang wajib memperoleh tingkat perlindungan lebih tinggi dibandingkan data pribadi pada umumnya. Rumah sakit sebagai badan hukum penyelenggara pelayanan kesehatan memiliki kewajiban untuk menjamin keamanan, kerahasiaan, integritas, dan ketersediaan data pasien melalui penerapan tata kelola perlindungan data yang memadai. Apabila terjadi kebocoran data akibat kelalaian rumah sakit, maka rumah sakit dapat dimintai pertanggungjawaban secara administratif, perdata, bahkan pidana sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

Meskipun kerangka regulasi mengenai perlindungan data pribadi telah berkembang secara signifikan, implementasinya masih menghadapi berbagai persoalan. Banyak rumah sakit belum memiliki tata kelola keamanan informasi yang memadai, pengawasan terhadap akses data masih lemah, penggunaan pihak ketiga dalam pengelolaan sistem elektronik belum sepenuhnya disertai mekanisme pengawasan yang efektif, serta belum terdapat standar pertanggungjawaban hukum yang secara komprehensif mengatur tanggung jawab rumah sakit apabila terjadi kebocoran data pasien. Kondisi tersebut menunjukkan adanya kesenjangan antara perkembangan digitalisasi pelayanan kesehatan dengan efektivitas perlindungan hukum terhadap privasi pasien.

Penelitian-penelitian terdahulu pada umumnya lebih banyak membahas perlindungan data pribadi dari perspektif hukum siber atau implementasi Undang-Undang Pelindungan Data Pribadi secara umum. Sementara itu, kajian yang secara khusus menganalisis pertanggungjawaban hukum rumah sakit sebagai badan hukum atas pelanggaran privasi pasien akibat kebocoran data elektronik masih relatif terbatas. Padahal, karakteristik hubungan hukum antara pasien, rumah sakit, tenaga kesehatan, penyedia sistem elektronik, dan pihak ketiga menimbulkan persoalan hukum yang kompleks mengenai pembebanan tanggung jawab, bentuk perlindungan hukum yang dapat diberikan kepada pasien, serta mekanisme pemulihan hak korban kebocoran data kesehatan.

Berdasarkan kondisi tersebut, penelitian ini menjadi penting untuk mengkaji secara komprehensif konsep perlindungan hukum terhadap privasi pasien dalam era digital serta menganalisis bentuk pertanggungjawaban hukum rumah sakit sebagai badan hukum apabila terjadi kebocoran data elektronik pasien. Kajian ini diharapkan dapat memberikan kontribusi terhadap pengembangan hukum kesehatan dan hukum pelindungan data pribadi di Indonesia sekaligus menjadi rekomendasi bagi pembentukan kebijakan yang mampu mewujudkan sistem pelayanan kesehatan digital yang aman, akuntabel, serta menjamin penghormatan terhadap hak privasi setiap pasien.

B. Rumusan Masalah

Dalam penelitian ini, yang menjadi permasalahan yang diajukan untuk dianalisis dirumuskan, Bagaimana Prinsip Kepailitan di Indonesia?

II. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan deskriptif. Penelitian hukum normatif dipilih karena penelitian ini



berfokus pada pengkajian norma-norma hukum yang di Indonesia.

III. PEMBAHASAN

Privasi pasien merupakan hak pasien untuk memperoleh perlindungan atas informasi pribadi dan informasi kesehatannya agar tidak diketahui, digunakan, diakses, atau disebarluaskan oleh pihak yang tidak berwenang. Makna privasi pasien tidak hanya berkaitan dengan kerahasiaan identitas, tetapi juga mencakup perlindungan terhadap kondisi kesehatan, riwayat penyakit, diagnosis, hasil pemeriksaan, tindakan medis, penggunaan obat, serta informasi lain yang diperoleh dalam hubungan pelayanan kesehatan. Hak privasi pasien lahir dari penghormatan terhadap martabat manusia, hak atas perlindungan diri pribadi, dan hak pasien untuk mengendalikan informasi yang melekat pada dirinya. Data kesehatan memiliki karakter sensitif karena dapat memengaruhi reputasi, relasi sosial, pekerjaan, dan kondisi psikologis pasien apabila disalahgunakan atau tersebar tanpa dasar hukum yang sah (Niffari, 2020).

Kedudukan privasi pasien dalam pelayanan kesehatan berkaitan erat dengan hubungan kepercayaan antara pasien dan tenaga kesehatan. Pasien memberikan informasi pribadi kepada dokter, perawat, rumah sakit, atau fasilitas pelayanan kesehatan dengan harapan bahwa informasi tersebut hanya digunakan untuk kepentingan pemeriksaan, pengobatan, perawatan, administrasi pelayanan, dan kepentingan hukum yang dibenarkan. Kewajiban menjaga privasi pasien melekat pada seluruh pihak yang terlibat dalam pelayanan kesehatan, termasuk rumah sakit sebagai penyelenggara layanan, tenaga medis, tenaga kesehatan, tenaga administrasi, serta pihak ketiga yang mengelola sistem elektronik rumah sakit. Pelanggaran terhadap privasi pasien dapat terjadi apabila informasi kesehatan diakses tanpa hak, digunakan di luar tujuan pelayanan, dibuka tanpa persetujuan, atau tidak dijaga dengan standar keamanan

yang memadai (Indra, Dewi, dan Wibowo, 2024).

Makna privasi pasien dalam era digital semakin luas karena informasi kesehatan tidak lagi hanya tersimpan dalam dokumen fisik, tetapi juga dalam rekam medis elektronik, sistem informasi rumah sakit, layanan telemedicine, aplikasi kesehatan, dan basis data elektronik. Perlindungan privasi pasien dalam sistem digital menuntut adanya pembatasan akses, persetujuan yang sah, keamanan sistem, pencatatan aktivitas pengguna, serta pengawasan terhadap setiap proses pengumpulan, penyimpanan, penggunaan, pengiriman, dan penghapusan data pasien. Kebocoran data elektronik rumah sakit dapat dikualifikasikan sebagai pelanggaran privasi pasien karena membuka kemungkinan penyalahgunaan informasi medis, pencurian identitas, diskriminasi, tekanan psikologis, dan hilangnya kepercayaan terhadap pelayanan kesehatan digital. Privasi pasien dalam konteks ini harus dipahami sebagai hak hukum yang wajib dilindungi oleh rumah sakit sebagai pengendali data dan badan hukum penyelenggara layanan kesehatan (Herisasono, 2024).

Hak privasi pasien dalam pelayanan kesehatan merupakan hak pasien untuk memperoleh perlindungan atas seluruh informasi pribadi dan data kesehatan yang diberikan, dikumpulkan, disimpan, atau diproses oleh fasilitas pelayanan kesehatan. Hak ini mencakup perlindungan terhadap identitas pasien, riwayat penyakit, diagnosis, hasil pemeriksaan laboratorium, tindakan medis, pengobatan, kondisi psikologis, serta informasi lain yang tercatat dalam rekam medis. Pasien berhak mendapatkan jaminan bahwa data kesehatannya hanya digunakan untuk kepentingan pelayanan kesehatan, administrasi medis, pembiayaan, penelitian yang sah, atau kepentingan hukum yang diperbolehkan oleh peraturan perundang-undangan. Rumah sakit sebagai penyelenggara



pelayanan kesehatan wajib menjaga kerahasiaan data pasien karena data kesehatan termasuk data pribadi spesifik yang memiliki tingkat sensitivitas tinggi dan dapat menimbulkan kerugian serius apabila disalahgunakan atau bocor kepada pihak yang tidak berwenang (UU PDP, 2022).

Hak pasien atas kerahasiaan rekam medis juga mencakup hak untuk mengetahui bagaimana data pribadinya digunakan, siapa pihak yang dapat mengaksesnya, tujuan pemrosesan data, serta dasar hukum pemrosesan data tersebut. Pasien tidak boleh diposisikan hanya sebagai objek pelayanan, tetapi juga sebagai subjek data yang memiliki hak atas informasi, persetujuan, akses, koreksi, pembatasan pemrosesan, serta perlindungan dari penyalahgunaan data kesehatan. Pengelolaan rekam medis elektronik harus dilakukan dengan prinsip kehati-hatian karena sistem digital memungkinkan data pasien diproses, dipindahkan, dibuka, dan disimpan dalam jaringan elektronik yang memiliki risiko keamanan. Pelanggaran terhadap hak privasi pasien terjadi apabila rekam medis dibuka tanpa dasar hukum, digunakan di luar tujuan pelayanan, disebarluaskan tanpa persetujuan, atau tidak diamankan secara layak oleh rumah sakit sebagai pengendali data (Indra, Dewi, dan Wibowo, 2024).

Data kesehatan merupakan bagian dari data pribadi spesifik karena memuat informasi yang berkaitan langsung dengan kondisi fisik, kondisi mental, riwayat penyakit, hasil pemeriksaan, diagnosis, tindakan medis, pengobatan, serta informasi lain yang menunjukkan keadaan kesehatan seseorang. Karakter data kesehatan berbeda dari data pribadi umum karena informasi yang terkandung di dalamnya dapat mengungkap keadaan paling pribadi dari pasien dan berpotensi menimbulkan kerugian serius apabila disebarluaskan tanpa hak. Data kesehatan dapat memperlihatkan penyakit tertentu, kondisi psikologis, riwayat perawatan,

hasil laboratorium, rekam medis, serta informasi medis yang dapat memengaruhi martabat, reputasi, hubungan sosial, pekerjaan, dan perlakuan masyarakat terhadap pasien. Kedudukan data kesehatan sebagai data pribadi spesifik menunjukkan bahwa data tersebut harus memperoleh perlindungan lebih tinggi dibandingkan data pribadi biasa (UU PDP, 2022).

Klasifikasi data kesehatan sebagai data pribadi spesifik menimbulkan kewajiban hukum bagi rumah sakit untuk menjaga keamanan, kerahasiaan, dan keabsahan setiap pemrosesan data pasien. Rumah sakit sebagai pengelola data kesehatan wajib memastikan bahwa data pasien hanya diakses oleh pihak yang berwenang, digunakan sesuai tujuan pelayanan kesehatan, diproses berdasarkan dasar hukum yang sah, dan dilindungi melalui sistem keamanan yang memadai. Kebocoran data kesehatan tidak hanya menimbulkan pelanggaran administratif, tetapi juga dapat menjadi pelanggaran privasi pasien karena informasi yang terbuka dapat digunakan untuk diskriminasi, penipuan, tekanan psikologis, atau penyalahgunaan identitas. Perlindungan terhadap data kesehatan dalam sistem rekam medis elektronik menjadi penting karena digitalisasi layanan kesehatan memperluas risiko akses tanpa hak, penyebaran tidak sah, dan kegagalan pengamanan data elektronik rumah sakit (Herisasono, 2024).

Bentuk pelanggaran privasi pasien dapat terjadi melalui berbagai tindakan yang menyebabkan informasi pribadi dan data kesehatan pasien diketahui, digunakan, diakses, atau disebarluaskan oleh pihak yang tidak berwenang. Akses tanpa izin merupakan salah satu bentuk pelanggaran yang terjadi ketika pegawai rumah sakit, tenaga kesehatan, tenaga administrasi, pihak ketiga, atau pihak luar membuka data pasien tanpa dasar hukum, tanpa kepentingan pelayanan, atau di luar kewenangan yang diberikan. Penyebaran data medis juga termasuk pelanggaran



privasi apabila informasi mengenai identitas pasien, diagnosis, hasil pemeriksaan, riwayat penyakit, tindakan medis, atau kondisi kesehatan disampaikan kepada pihak lain tanpa persetujuan pasien atau tanpa dasar hukum yang sah. Penggunaan data tanpa persetujuan menjadi pelanggaran apabila data pasien digunakan untuk kepentingan komersial, publikasi, penelitian, promosi, atau kepentingan lain yang tidak berkaitan langsung dengan pelayanan kesehatan dan tidak didasarkan pada persetujuan yang sah (UU PDP, 2022).

Kebocoran rekam medis elektronik merupakan bentuk pelanggaran privasi pasien yang semakin relevan dalam layanan kesehatan digital karena data pasien tersimpan dalam sistem elektronik yang rentan terhadap peretasan, kelalaian pengamanan, kesalahan konfigurasi, penggunaan akun bersama, atau lemahnya pengawasan akses. Penyalahgunaan informasi pasien dapat terjadi ketika data kesehatan dipakai untuk melakukan penipuan, diskriminasi, pemerasan, pencemaran nama baik, atau tindakan lain yang merugikan pasien secara ekonomi, sosial, maupun psikologis. Rumah sakit sebagai penyelenggara pelayanan kesehatan memiliki tanggung jawab untuk mencegah bentuk-bentuk pelanggaran tersebut melalui pembatasan akses, pengamanan sistem, audit penggunaan data, pelatihan pegawai, pengawasan vendor, dan penerapan standar perlindungan rekam medis elektronik. Pelanggaran privasi pasien dalam konteks rumah sakit tidak hanya menunjukkan adanya kerugian bagi pasien, tetapi juga dapat menjadi indikator kelalaian organisasi yang relevan dalam pembebanan pertanggungjawaban hukum terhadap rumah sakit sebagai badan hukum (Tampubolon, Putera, dan Huda, 2024).

Kerugian ekonomi merupakan salah satu dampak serius dari pelanggaran privasi pasien akibat kebocoran data kesehatan. Data pasien yang bocor dapat

digunakan untuk penipuan, pencurian identitas, klaim asuransi palsu, penyalahgunaan nomor identitas, pembukaan akun ilegal, atau tindakan lain yang menimbulkan kerugian finansial bagi pasien. Informasi kesehatan yang dikaitkan dengan data identitas, alamat, nomor telepon, data pembayaran, dan riwayat pelayanan medis memiliki nilai ekonomi tinggi karena dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk kepentingan komersial maupun kejahatan siber. Kebocoran data pasien juga dapat menimbulkan biaya tambahan bagi korban untuk memulihkan keamanan akun, mengganti dokumen, mengawasi penyalahgunaan identitas, atau menempuh mekanisme hukum guna memperoleh perlindungan dan pemulihan hak (IBM Security, 2024).

Dampak sosial dari pelanggaran privasi pasien dapat berupa diskriminasi, stigma, dan perlakuan tidak adil terhadap pasien. Informasi mengenai penyakit tertentu, kondisi mental, riwayat pengobatan, status reproduksi, penyakit menular, atau tindakan medis tertentu dapat memengaruhi cara keluarga, lingkungan kerja, lembaga pendidikan, perusahaan asuransi, atau masyarakat memperlakukan pasien. Data kesehatan yang tersebar tanpa hak dapat menimbulkan tekanan psikologis karena pasien merasa kehilangan kendali atas informasi pribadinya dan merasa tidak aman dalam menggunakan layanan kesehatan. Kondisi tersebut dapat menimbulkan rasa malu, kecemasan, ketakutan, trauma, dan penurunan kepercayaan diri, terutama apabila informasi medis yang bocor berkaitan dengan kondisi kesehatan yang sangat pribadi atau sensitif (Niffari, 2020).

Hilangnya rasa aman menjadi dampak penting dari pelanggaran privasi pasien karena hubungan antara pasien dan rumah sakit dibangun atas dasar kepercayaan. Pasien akan lebih berhati-hati atau bahkan enggan menyampaikan informasi kesehatan secara jujur apabila merasa data



pribadinya tidak terlindungi dengan baik. Penurunan kepercayaan terhadap layanan kesehatan digital dapat menghambat pemanfaatan rekam medis elektronik, telemedicine, aplikasi kesehatan, dan sistem informasi rumah sakit. Dampak tersebut tidak hanya merugikan pasien secara individual, tetapi juga mengganggu efektivitas pelayanan kesehatan karena data yang tidak lengkap atau tidak akurat dapat memengaruhi diagnosis, pengobatan, dan kesinambungan pelayanan medis. Kebocoran data pasien menunjukkan bahwa pelanggaran privasi dalam layanan kesehatan digital memiliki akibat hukum, sosial, ekonomi, dan psikologis yang perlu dipertimbangkan dalam pertanggungjawaban rumah sakit sebagai badan hukum (Tampubolon, Putera, dan Huda, 2024).

Perlindungan hukum terhadap privasi pasien merupakan bentuk jaminan agar informasi pribadi dan data kesehatan pasien tidak digunakan, diakses, disimpan, atau disebarluaskan secara sewenang-wenang oleh pihak yang tidak berwenang. Regulasi kesehatan memberikan dasar bahwa pasien berhak memperoleh pelayanan yang menghormati kerahasiaan kondisi kesehatan, riwayat penyakit, diagnosis, tindakan medis, serta data yang tercantum dalam rekam medis. Data kesehatan juga memperoleh perlindungan khusus dalam rezim perlindungan data pribadi karena termasuk data pribadi spesifik yang memiliki sensitivitas tinggi dan dapat menimbulkan kerugian serius apabila bocor atau disalahgunakan. Perlindungan tersebut menempatkan rumah sakit sebagai pihak yang wajib menjaga kerahasiaan rekam medis, menjamin keamanan pengelolaan data pasien, serta memastikan pemrosesan data dilakukan berdasarkan dasar hukum yang sah (UU PDP, 2022).

Implementasi perlindungan hukum terhadap privasi pasien dalam layanan kesehatan digital harus dilakukan melalui penguatan regulasi rekam medis, perlindungan data pribadi, dan pengamanan

sistem elektronik. Rumah sakit yang menggunakan rekam medis elektronik dan sistem informasi rumah sakit wajib menerapkan pembatasan akses, pengamanan data, pencatatan aktivitas pengguna, pengawasan terhadap pihak ketiga, serta mekanisme pelaporan apabila terjadi kebocoran data. Kewajiban tersebut penting karena digitalisasi pelayanan kesehatan memperbesar risiko akses tanpa izin, penyebaran data medis, penggunaan data tanpa persetujuan, dan penyalahgunaan informasi pasien. Perlindungan hukum terhadap privasi pasien tidak hanya bersifat administratif, tetapi juga dapat berhubungan dengan pertanggungjawaban perdata, administratif, dan pidana apabila kebocoran data terjadi akibat kelalaian rumah sakit sebagai badan hukum penyelenggara layanan kesehatan (Indra, Dewi, dan Wibowo, 2024).

Data elektronik rumah sakit merupakan seluruh informasi digital yang dikumpulkan, disimpan, dikelola, dikirim, digunakan, dan diproses melalui sistem elektronik dalam penyelenggaraan pelayanan kesehatan. Data tersebut dapat meliputi identitas pasien, nomor rekam medis, riwayat penyakit, diagnosis, hasil laboratorium, hasil radiologi, tindakan medis, resep obat, data pembayaran, data asuransi, data administrasi, serta informasi lain yang berkaitan dengan pelayanan rumah sakit. Data elektronik rumah sakit tidak hanya berfungsi sebagai catatan administratif, tetapi juga sebagai dasar pelayanan medis, kesinambungan perawatan, pengambilan keputusan klinis, pembuktian hukum, pelaporan kesehatan, dan evaluasi mutu layanan. Penggunaan rekam medis elektronik menjadikan data pasien tersimpan dalam bentuk digital sehingga pengelolaannya harus dilakukan secara aman, tertib, akurat, dan bertanggung jawab oleh fasilitas pelayanan kesehatan (Permenkes Rekam Medis, 2022).

Kedudukan data elektronik rumah sakit dalam layanan kesehatan digital



berkaitan erat dengan sistem informasi rumah sakit, rekam medis elektronik, telemedicine, aplikasi kesehatan, dan basis data pelayanan kesehatan. Data elektronik tersebut dapat dikualifikasikan sebagai informasi elektronik dan dokumen elektronik karena dibuat, diterima, dikirim, disimpan, atau diproses melalui perangkat dan sistem elektronik. Pengelolaan data elektronik rumah sakit harus memperhatikan prinsip keamanan, kerahasiaan, integritas, ketersediaan, keaslian, serta pembatasan akses agar tidak terjadi penyalahgunaan atau kebocoran data pasien. Data elektronik rumah sakit memiliki nilai hukum dan nilai perlindungan yang tinggi karena sebagian besar memuat data kesehatan sebagai data pribadi spesifik yang wajib dilindungi oleh rumah sakit sebagai pengendali data dan badan hukum penyelenggara pelayanan kesehatan (UU PDP, 2022).

Ruang lingkup data elektronik rumah sakit mencakup seluruh informasi digital yang dihasilkan, dikumpulkan, disimpan, dan diproses dalam penyelenggaraan pelayanan kesehatan. Data tersebut meliputi data identitas pasien, nomor rekam medis, alamat, nomor identitas kependudukan, nomor kontak, data keluarga, data dokter penanggung jawab, serta data administrasi pendaftaran pasien. Ruang lingkup berikutnya mencakup rekam medis elektronik yang berisi anamnesis, diagnosis, riwayat penyakit, tindakan medis, resep obat, catatan perkembangan pasien, ringkasan pulang, hasil konsultasi, serta informasi klinis lain yang berkaitan langsung dengan kondisi kesehatan pasien. Hasil laboratorium, hasil radiologi, catatan pemeriksaan penunjang, dan data tindakan medis juga termasuk data elektronik rumah sakit karena menjadi bagian dari proses pelayanan, pembuktian medis, dan kesinambungan perawatan pasien (Permenkes Rekam Medis, 2022).

Data elektronik rumah sakit juga mencakup data pembayaran, data asuransi, data klaim BPJS atau penjamin lain, data

rujukan, data persetujuan tindakan medis, data persetujuan pemrosesan data, serta data administrasi pelayanan kesehatan. Data pembayaran dan asuransi mungkin tidak selalu berisi diagnosis secara langsung, tetapi data tersebut tetap dapat menunjukkan hubungan pasien dengan layanan kesehatan tertentu dan dapat mengungkap kondisi kesehatan apabila dikaitkan dengan rekam medis elektronik. Data elektronik rumah sakit juga meliputi metadata dan jejak akses sistem, seperti waktu akses, identitas pengguna, perubahan data, riwayat pengiriman dokumen, dan aktivitas pengguna dalam sistem informasi rumah sakit. Ruang lingkup yang luas tersebut menunjukkan bahwa data elektronik rumah sakit harus diperlakukan sebagai aset hukum dan aset informasi yang wajib dilindungi melalui pembatasan akses, pengamanan sistem, pengawasan internal, serta tata kelola perlindungan data pribadi yang ketat (Siregar dan Sinaga, 2025).

Rekam medis elektronik merupakan dokumen digital yang memuat informasi mengenai identitas pasien, hasil pemeriksaan, diagnosis, tindakan medis, terapi, pengobatan, perkembangan kondisi pasien, serta seluruh riwayat pelayanan kesehatan yang diberikan oleh fasilitas pelayanan kesehatan. Kedudukan rekam medis elektronik sebagai bagian dari data elektronik rumah sakit menunjukkan bahwa informasi kesehatan pasien tidak lagi hanya dikelola dalam bentuk dokumen fisik, tetapi juga diproses melalui sistem informasi dan perangkat elektronik. Rekam medis elektronik memiliki fungsi medis karena menjadi dasar bagi tenaga kesehatan dalam menentukan diagnosis, merencanakan tindakan, memberikan terapi, memantau perkembangan pasien, dan menjamin kesinambungan pelayanan kesehatan. Rekam medis elektronik juga menjadi instrumen penting dalam peningkatan mutu pelayanan karena data yang tersimpan secara digital dapat membantu rumah sakit melakukan evaluasi pelayanan, koordinasi antarunit,



serta pengambilan keputusan klinis yang lebih cepat dan akurat (Permenkes Rekam Medis, 2022).

Fungsi administratif, hukum, dan pembuktian dari rekam medis elektronik menjadikan dokumen ini memiliki kedudukan penting dalam pelayanan kesehatan digital. Rekam medis elektronik berfungsi secara administratif karena digunakan untuk pendaftaran pasien, pengelolaan pelayanan, pelaporan, pembiayaan, klaim asuransi, dan dokumentasi kegiatan rumah sakit. Rekam medis elektronik memiliki fungsi hukum karena dapat menunjukkan adanya hubungan hukum antara pasien, tenaga kesehatan, dan rumah sakit, serta dapat menjadi dasar penilaian terhadap kesesuaian tindakan medis dengan standar pelayanan. Rekam medis elektronik juga memiliki fungsi pembuktian karena informasi yang tersimpan di dalamnya dapat digunakan dalam penyelesaian sengketa medis, pemeriksaan administratif, audit pelayanan, atau proses hukum apabila terjadi dugaan pelanggaran hak pasien. Kedudukan rekam medis elektronik sebagai dokumen digital yang memuat data kesehatan spesifik menuntut rumah sakit untuk menjamin kerahasiaan, keutuhan, keaslian, keamanan, dan keterbatasan akses terhadap data pasien (Siregar dan Sinaga, 2025).

Pengelolaan data elektronik dalam sistem informasi rumah sakit merupakan proses yang mencakup pengumpulan, pencatatan, penyimpanan, penggunaan, pengiriman, pengamanan, dan penghapusan data pasien secara terstruktur melalui perangkat dan sistem elektronik. Pengumpulan data pasien dilakukan sejak tahap pendaftaran, pemeriksaan, tindakan medis, pemberian obat, pemeriksaan laboratorium, klaim pembiayaan, sampai dengan pelayanan lanjutan. Penyimpanan data dilakukan dalam sistem informasi rumah sakit dan rekam medis elektronik agar informasi pasien dapat digunakan untuk kesinambungan pelayanan, evaluasi mutu, administrasi kesehatan, serta

kepentingan hukum yang sah. Penggunaan data pasien harus dibatasi pada tujuan pelayanan kesehatan, administrasi rumah sakit, pelaporan yang diperbolehkan, dan kepentingan lain yang memiliki dasar hukum agar tidak terjadi penyalahgunaan informasi pribadi pasien (Permenkes Rekam Medis, 2022).

Pengiriman, pengamanan, dan penghapusan data pasien merupakan bagian penting dari tata kelola data elektronik rumah sakit karena setiap proses pemindahan atau akses data memiliki risiko kebocoran. Pengiriman data pasien kepada pihak lain, seperti laboratorium, dokter rujukan, penjamin pembiayaan, atau otoritas yang berwenang, harus dilakukan berdasarkan kewenangan, persetujuan, atau ketentuan hukum yang sah. Pengamanan data dilakukan melalui pembatasan akses, autentikasi pengguna, enkripsi, pencatatan aktivitas sistem, audit internal, pengawasan vendor, dan prosedur respons insiden apabila terjadi gangguan keamanan. Penghapusan data pasien harus dilakukan sesuai ketentuan retensi, kepentingan hukum, dan prinsip perlindungan data pribadi agar data yang tidak lagi diperlukan tidak disimpan secara berlebihan atau digunakan di luar tujuan yang sah (UU PDP, 2022).

Resiko kebocoran data elektronik rumah sakit dapat muncul dari berbagai bentuk ancaman keamanan siber yang menyerang sistem informasi, rekam medis elektronik, basis data pasien, dan jaringan internal rumah sakit. Peretasan menjadi salah satu risiko utama karena pihak luar dapat berusaha masuk ke sistem rumah sakit untuk mengambil data identitas pasien, riwayat penyakit, hasil pemeriksaan, data pembayaran, atau informasi medis lain yang memiliki nilai tinggi. Ransomware juga menjadi ancaman serius karena dapat mengenkripsi data rumah sakit, melumpuhkan akses terhadap rekam medis elektronik, mengganggu pelayanan kesehatan, dan memaksa rumah sakit membayar tebusan



untuk memulihkan sistem. Phishing dapat menargetkan pegawai rumah sakit melalui pesan palsu, tautan berbahaya, atau lampiran yang dirancang untuk mencuri kredensial pengguna sehingga pelaku dapat mengakses sistem elektronik secara tidak sah (BSSN, 2024).

Akses internal tanpa izin, lemahnya pengendalian akses, dan kelalaian pihak ketiga juga menjadi sumber risiko kebocoran data elektronik rumah sakit. Pegawai yang memiliki akses berlebihan, penggunaan akun bersama, kata sandi lemah, tidak adanya autentikasi berlapis, serta minimnya pencatatan aktivitas pengguna dapat membuka peluang penyalahgunaan data pasien dari dalam organisasi. Pihak ketiga seperti vendor sistem informasi, penyedia layanan komputasi awan, pengembang aplikasi, laboratorium rekanan, atau penyedia layanan telemedicine juga dapat menjadi titik lemah apabila kontrak, audit, dan standar keamanan tidak diatur secara tegas. Risiko kebocoran data elektronik rumah sakit menunjukkan bahwa perlindungan data pasien tidak cukup hanya mengandalkan teknologi, tetapi juga membutuhkan tata kelola, pengawasan internal, pelatihan pegawai, manajemen risiko, dan tanggung jawab hukum rumah sakit sebagai pengendali data (Siregar dan Sinaga, 2025).

Standar keamanan data elektronik rumah sakit merupakan seperangkat langkah teknis dan organisatoris yang bertujuan melindungi kerahasiaan, keutuhan, ketersediaan, dan keaslian data pasien. Enkripsi diperlukan untuk melindungi data pasien saat disimpan maupun dikirim agar informasi medis tidak mudah dibaca oleh pihak yang tidak berwenang. Autentikasi berlapis diperlukan untuk memastikan bahwa hanya pengguna yang benar-benar memiliki kewenangan yang dapat mengakses sistem informasi rumah sakit. Pembatasan akses berbasis peran juga penting karena setiap tenaga medis, tenaga kesehatan, tenaga administrasi, vendor,

atau pihak lain hanya boleh mengakses data sesuai kebutuhan tugasnya. Audit log diperlukan untuk mencatat aktivitas pengguna, perubahan data, waktu akses, dan jejak penggunaan sistem sehingga rumah sakit dapat menelusuri sumber kesalahan atau pelanggaran apabila terjadi kebocoran data (NIST, 2024).

Pengawasan terhadap pencadangan data, vendor, dan manajemen risiko keamanan siber juga menjadi bagian penting dari standar keamanan data elektronik rumah sakit. Pencadangan data diperlukan agar rekam medis elektronik dan data pelayanan tetap dapat dipulihkan apabila terjadi kerusakan sistem, serangan ransomware, bencana, atau gangguan operasional. Pengawasan vendor diperlukan karena rumah sakit sering menggunakan pihak ketiga dalam pengembangan aplikasi, penyimpanan data, pemeliharaan sistem, atau layanan komputasi awan. Manajemen risiko keamanan siber harus dilakukan melalui identifikasi aset data, penilaian ancaman, evaluasi kerentanan, penetapan kontrol keamanan, pemantauan berkala, dan respons insiden. Standar keamanan tersebut menjadi ukuran penting untuk menilai apakah rumah sakit telah menjalankan kewajiban perlindungan data pasien secara layak dan bertanggung jawab (ISO/IEC 27001, 2022).

IV. KESIMPULAN

Perlindungan privasi pasien merupakan bagian dari hak asasi manusia yang harus dijamin dalam setiap penyelenggaraan pelayanan kesehatan, terutama di era digital ketika rekam medis dan data kesehatan dikelola melalui sistem elektronik. Data kesehatan sebagai data pribadi spesifik memiliki tingkat sensitivitas yang tinggi sehingga memerlukan perlindungan hukum yang lebih ketat dibandingkan data pribadi pada umumnya. Digitalisasi pelayanan kesehatan melalui rekam medis elektronik dan sistem informasi rumah sakit memang meningkatkan efektivitas pelayanan,



namun pada saat yang sama juga memperbesar risiko kebocoran, akses tanpa hak, penyalahgunaan data, dan berbagai bentuk kejahatan siber yang dapat menimbulkan kerugian ekonomi, sosial, psikologis, maupun hilangnya kepercayaan masyarakat terhadap institusi pelayanan kesehatan.

Secara normatif, Indonesia telah memiliki landasan hukum yang cukup memadai melalui Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Peraturan Menteri Kesehatan mengenai Rekam Medis Elektronik, serta berbagai regulasi yang mengatur penyelenggaraan sistem elektronik. Keseluruhan regulasi tersebut menempatkan rumah sakit sebagai pengendali data yang berkewajiban menjaga kerahasiaan, keamanan, integritas, dan ketersediaan data pasien melalui penerapan tata kelola keamanan informasi yang efektif. Apabila terjadi kebocoran data akibat kelalaian atau kegagalan rumah sakit dalam memenuhi kewajiban tersebut, maka rumah sakit dapat dimintai pertanggungjawaban secara administratif, perdata, maupun pidana

sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

Meskipun demikian, implementasi perlindungan privasi pasien masih menghadapi berbagai tantangan, antara lain lemahnya tata kelola keamanan informasi, belum optimalnya pengawasan terhadap akses data, meningkatnya ancaman serangan siber, serta keterlibatan pihak ketiga dalam pengelolaan sistem elektronik yang belum sepenuhnya disertai mekanisme pengawasan yang memadai. Oleh karena itu, diperlukan penguatan regulasi, peningkatan standar keamanan sistem informasi rumah sakit, penerapan prinsip akuntabilitas dalam pengelolaan data pribadi, serta pengawasan yang lebih efektif agar perlindungan terhadap privasi pasien tidak hanya menjadi kewajiban normatif, tetapi juga dapat diwujudkan secara nyata dalam praktik pelayanan kesehatan digital. Dengan demikian, keseimbangan antara pemanfaatan teknologi informasi di bidang kesehatan dan perlindungan hak privasi pasien dapat tercapai secara optimal dalam mewujudkan sistem pelayanan kesehatan yang aman, terpercaya, dan berkeadilan.

DAFTAR PUSTAKA

- Ashworth, A., & Horder, J. *Principles of Criminal Law* (10th ed.). Oxford University Press, 2022.
- Ayiliani, Fanisa Mayda, dan Elfia Farida. "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara." *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431–455.
- Badan Siber dan Sandi Negara. *Laporan Tahunan Keamanan Siber Indonesia 2024*. 2024. <https://bssn.go.id>
- Baldwin, R., Cave, M., & Lodge, M. *Understanding Regulation: Theory, Strategy, and Practice* (3rd ed.). Oxford University Press, 2022.
- Bennett, C. J., & Raab, C. D. *The Governance of Privacy: Policy Instruments in Global Perspective* (2nd ed.). MIT Press, 2020.
- Budhijanto, Danrivanto. *Hukum Kontrak Digital*. Bandung: Logoz Publishing, 2024.
- Budhijanto, Danrivanto. *Hukum Pelindungan Data Pribadi di Indonesia: Cyberlaw & Cybersecurity*. Bandung: Refika Aditama, 2023.
- Budhijanto, Danrivanto. *Revolusi Cyberlaw Indonesia: Revisi UU ITE 2024, Kedaulatan Digital dan Kecerdasan Artifisial*. Bandung: Logoz Publishing, 2024.
- Budiyanto, S. H. *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia*. Sada Kurnia Pustaka, 2025.



- Creswell, J. W. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). SAGE Publications, 2021.
- Creswell, J. W., & Creswell, J. D. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (6th ed.). SAGE Publications, 2022.
- CyberPeace Institute. *The Cyber Threat Landscape in the Healthcare Sector*. 2022. <https://cyberpeaceinstitute.org/publications/the-cyber-threat-landscape-in-the-healthcare-sector/>
- Daeng, Y., Ningsih, N., Khairul, F., Winarsih, S., & Zulaida. "Pertanggungjawaban Pidana Rumah Sakit dan Tenaga Medis di Atas Tindakan Malpraktik Berdasarkan Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan." *INNOVATIVE: Journal of Social Science Research* 3, no. 6 (2023).
- Duff, R. A., Farmer, L., Marshall, S., Renzo, M., & Tadros, V. *The Boundaries of the Criminal Law*. Oxford University Press, 2022.
- European Union Agency for Cybersecurity (ENISA). *Threat Landscape 2023: Health Sector*. 2023. <https://www.enisa.europa.eu/publications/threat-landscape-2023-health-sector>
- Gani, T. A. *Kedaulatan Data Digital untuk Integritas Bangsa*. Banda Aceh: Syiah Kuala University Press, 2023.
- Gobert, J., & Punch, M. *Rethinking Corporate Crime*. Cambridge University Press, 2021.
- Greenleaf, G. "Global Data Privacy Laws 2022: Despite COVID Delays, 157 Laws Show GDPR Dominance." *Privacy Laws & Business International Report* (2022).
- Hariri, A., Wahyuni, W., & Rochmat, A. "Menghadapi Transformasi Digital Layanan Kesehatan." (2025).
- Herisasono, Adi. "Perlindungan Hukum terhadap Privasi Data Pasien dalam Sistem Rekam Medis Elektronik." *Jurnal Kolaboratif Sains* 7, no. 12 (2024): 4677–4681.
- Hiariej, Eddy O. S. *Prinsip-Prinsip Hukum Pidana: Edisi Penyesuaian KUHP Nasional*. Depok: Rajawali Pers, 2024.
- Husak, D. *The Philosophy of Criminal Law: Selected Essays*. Oxford University Press, 2021.
- IBM Security. *Cost of a Data Breach Report 2023*. 2023. <https://www.ibm.com/reports/data-breach>
- Ibrahim, J. *Teori dan Metodologi Penelitian Hukum Normatif*. Bayumedia Publishing, 2020.
- Ilyas, Adam. *Hukum Pidana Baru Indonesia: Penjelasan Lengkap Mengenai Aturan Umum KUHP Baru*. Depok: Rajawali Pers, 2024.
- Indarta, Yose. *Cyber Law: Dimensi Hukum dalam Era Digital*. Pustaka Galeri Mandiri, 2025.
- Indra, Indra, Trihoni Nalesti Dewi, dan Daniel Budi Wibowo. "Perlindungan Kerahasiaan Data Pasien vs Kewajiban Membuka Akses Rekam Medis Elektronik." *Soepra Jurnal Hukum Kesehatan* 10, no. 1 (2024): 97–117.
- Kementerian Kesehatan Republik Indonesia. *Transformasi Digital Kesehatan Indonesia*. 2023. <https://www.kemkes.go.id>
- Kementerian Komunikasi dan Informatika. "Siaran Pers Terkait Dugaan Kebocoran Data BPJS Kesehatan." 2021.
- Kristian. *Hukum Pidana Korporasi: Teori dan Perkembangannya di Indonesia*. Kencana, 2022.
- Kuner, C. "The GDPR and Private International Law." *International Data Privacy Law* 11, no. 1 (2021).
- Lestari, R. "Tanggung Jawab Rumah Sakit atas Kebocoran Rekam Medis Elektronik." *Jurnal Hukum Kesehatan* 9, no. 2 (2023).
- Malau, Parningotan, dan Syahlan. *Criminal Act, Criminal Liability & Punishment terhadap Korporasi dalam KUHP Baru dan Undang-Undang Khusus serta Tantangan Penegakan Hukumnya*. Padang: Media Penerbit Indonesia, 2024.
- Marzuki, P. M. *Penelitian Hukum*. Kencana, 2021.



- McLeod, A., & Dolezel, D. "Cyber-Analytics: Modeling Factors Associated with Healthcare Data Breaches." *Decision Support Systems* 147 (2021).
- Ministry of Communication and Information Technology (Kominfo). "Indonesia Digital Talent Outlook." 2024.
- Niffari, Hanifan. "Perlindungan Data Pribadi sebagai Bagian dari Hak Asasi Manusia atas Perlindungan Diri Pribadi: Suatu Tinjauan Komparatif dengan Peraturan Perundang-Undangan di Negara Lain." *Jurnal Yuridis* 7, no. 1 (2020): 105–119.
- Organisation for Economic Co-operation and Development (OECD). *Health Data Governance for the Digital Age*. 2020. <https://www.oecd.org/health/health-data-governance-for-the-digital-age-8b53c6c0-en.htm>
- Parker, C., & Nielsen, V. L. *Explaining Compliance: Business Responses to Regulation*. Edward Elgar Publishing, 2021.
- Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis.
- Peraturan Menteri Kesehatan Republik Indonesia Nomor 4 Tahun 2023 tentang Standar Pelayanan Minimal Bidang Kesehatan.
- Pratama, A., & Wijaya, D. "Perlindungan Data Medis dalam Perspektif Hukum Siber Indonesia." *Jurnal Legislasi Indonesia* 19, no. 3 (2022).
- Putra, Moody Rizqy Syailendra. *Hukum Perlindungan Data Pribadi di Indonesia*. Depok: Rajawali Pers, 2025.
- Rahman, Faiz. "Kerangka Hukum Perlindungan Data Pribadi dalam Penerapan Sistem Pemerintahan Berbasis Elektronik di Indonesia." *Jurnal Legislasi Indonesia* 18, no. 1 (2021): 81–102.
- Republik Indonesia. *Kitab Undang-Undang Hukum Perdata (KUHPerdata)*, 1947.
- Republik Indonesia. *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*.
- Republik Indonesia. *Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan*, Lembaran Negara Republik Indonesia Tahun 2023 Nomor 99.
- Republik Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.
- Santos, Ricardo, dan Vientje Ratna Multiwijaya. "Tanggung Jawab Korporasi dalam Kasus Kebocoran Data serta Implikasinya terhadap Ekonomi Digital." *Ensiklopedia Sosial Review* 6, no. 3 (2024): 103–109.
- Schabas, W. A. *International Human Rights Law and Data Protection*. Cambridge University Press, 2023.
- Setiawan, I. "Implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia." *Jurnal Rechtsvinding* 12, no. 2 (2023).
- Simanjuntak, P. H. "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.
- Simester, A. P., & Sullivan, G. R. *Criminal Law: Theory and Doctrine* (8th ed.). Hart Publishing, 2022.
- Siregar, H. "Tata Kelola Keamanan Siber pada Sistem Informasi Kesehatan Nasional." *Jurnal Teknologi Informasi dan Hukum* 6, no. 1 (2024).
- Soekanto, S., & Mamudji, S. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Edisi Revisi). Rajawali Pers, 2020.
- Soekanto, S., & Mamudji, S. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. RajaGrafindo Persada, 2022.
- Solove, D. J. *Understanding Privacy*. Harvard University Press, 2021.



- Susanto, A., & Ramli, A. "Pertanggungjawaban Pidana Korporasi dalam Pelanggaran Data Pribadi di Indonesia." *Jurnal Hukum & Pembangunan* 53, no. 2 (2023).
- Syailendra, Moody Rizqy, Gunardi Lie, dan Ahmad Sudiro. "Personal Data Protection Law in Indonesia: Challenges and Opportunities." *Indonesia Law Review* 14, no. 2 (2024).
- Tampubolon, Erwin Tumpal Ferdinand, Andika Persada Putera, dan M. Khoirul Huda. "Pertanggungjawaban Hukum Rumah Sakit Terkait Kebocoran Data Pribadi Pasien Berdasarkan Peraturan Perundang-Undangan." *Syntax Idea* 6, no. 3 (2024): 1388–1402.
- U.S. Department of Health and Human Services. *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*. 2024.
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- United Nations Human Rights Council. *The Right to Privacy in the Digital Age*. 2022.
- Verizon. *Data Breach Investigations Report* 2024. 2024.
<https://www.verizon.com/business/resources/reports/dbir/>
- Watkut, Fransiscus Xaverius, Muhammad Toha Ingratubun, Muhammad Hafiz Ingsaputro, dan Arie Tri Hartantyo. "Pertanggungjawaban Pidana Pengendali Data Pribadi terhadap Kebocoran Data Pribadi Warga Negara Indonesia." *Jurnal Hukum Ius Publicum* 5, no. 2 (2024): 177–198.
- Wells, C. *Corporations and Criminal Responsibility* (2nd ed.). Oxford University Press, 2020.
- World Bank. Malpass, David. *Remarks at the Human Capital Conclave*. 2021.
<https://doi.org/10.1596/35399>
- World Health Organization. *Ethics and Governance of Artificial Intelligence for Health*. WHO Press, 2021.
- World Health Organization. *Global Patient Safety Action Plan 2021–2030*. 2021.
- World Health Organization. *Global Strategy on Digital Health 2020–2025 Progress Report*. 2023.
- World Health Organization. *Health Financing for Universal Health Coverage*. 2022.
- World Health Organization. *Patient Safety Framework*. 2023.