

Hak atas Keamanan dan Kerahasiaan Data Medis Pasien dalam Konsultasi Kesehatan Online

Adelina Mariani Simatupang^{1*}, Rospita Adelina Siregar²

Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Kristen Indonesia, Indonesia

E-mail: adelina.mariani80@gmail.com¹, rospita.siregar@uki.ac.id²

Article History:

Received: 01 Januari 2026

Revised: 19 Januari 2026

Accepted: 22 Januari 2026

Keywords:

Online Consultation Services, Medical Records, Patient Data Security and Confidentiality.

Abstract: The development of information technology has driven a significant transformation in the healthcare system through online health consultation services. These services provide easy access for the public, but also pose new legal challenges, particularly regarding the protection of the security and confidentiality of patient medical data. Medical data is highly sensitive personal data because it is directly related to a person's health, identity, and dignity, thus requiring strict legal protection. This study aims to analyze the regulation and implementation of legal protection for the right to security and confidentiality of patient medical data in online health consultation services in Indonesia, identify legal issues encountered in their implementation, and examine legal and policy efforts that have been and need to be implemented to ensure such protection effectively and sustainably. The research method used is normative legal research with a statutory and conceptual approach, through analysis of primary, secondary, and tertiary legal materials. The results show that the protection of patient medical data is normatively regulated in Law Number 27 of 2022 concerning Personal Data Protection, Law Number 17 of 2023 concerning Health, and the Law on Information and Electronic Transactions. However, these regulations remain partial and incompletely harmonized, creating legal loopholes, particularly regarding technical security standards, the division of responsibilities between parties, the management of electronic medical records, and oversight mechanisms. Therefore, strengthening more specific regulations, improving inter-agency coordination, and enhancing human resource capacity are needed to ensure optimal legal protection of patient medical data in online health consultation services without hindering innovation in digital health services.

Kata Kunci: Pelayanan Konsultasi Online, Rekam Medis, Keamanan dan Kerahasiaan Data Pasien.

Abstrak: Perkembangan teknologi informasi telah mendorong transformasi signifikan dalam sistem pelayanan kesehatan melalui layanan konsultasi kesehatan online. Layanan ini memberikan kemudahan akses bagi masyarakat, namun sekaligus menimbulkan tantangan

hukum baru, khususnya terkait perlindungan atas keamanan dan kerahasiaan data medis pasien. Data medis merupakan data pribadi yang sangat sensitif karena berkaitan langsung dengan kondisi kesehatan, identitas, serta martabat seseorang, sehingga memerlukan perlindungan hukum yang ketat. Penelitian ini bertujuan untuk menganalisis pengaturan dan pelaksanaan perlindungan hukum terhadap hak atas keamanan dan kerahasiaan data medis pasien dalam layanan konsultasi kesehatan online di Indonesia, mengidentifikasi permasalahan hukum yang dihadapi dalam penerapannya, serta mengkaji upaya hukum dan kebijakan yang telah dan perlu dilakukan untuk menjamin perlindungan tersebut secara efektif dan berkelanjutan. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan peraturan perundang-undangan dan konseptual, melalui analisis bahan hukum primer, sekunder, dan tersier. Hasil penelitian menunjukkan bahwa perlindungan data medis pasien secara normatif telah diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, serta Undang-Undang Informasi dan Transaksi Elektronik. Namun demikian, pengaturan tersebut masih bersifat parsial dan belum sepenuhnya harmonis, sehingga menimbulkan celah hukum, terutama terkait standar teknis keamanan, pembagian tanggung jawab para pihak, pengelolaan rekam medis elektronik, dan mekanisme pengawasan. Oleh karena itu, diperlukan penguatan regulasi yang lebih spesifik, peningkatan koordinasi antarinstansi, serta penguatan kapasitas sumber daya manusia agar perlindungan hukum terhadap data medis pasien dalam layanan konsultasi kesehatan online dapat terwujud secara optimal tanpa menghambat inovasi pelayanan kesehatan digital.

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transformasi dalam sistem pelayanan kesehatan, salah satunya melalui layanan konsultasi kesehatan online atau disebut juga konsultasi kesehatan online. Model layanan ini memungkinkan pasien memperoleh konsultasi medis secara cepat tanpa dibatasi ruang dan waktu. Namun, kemudahan tersebut memunculkan persoalan hukum baru, terutama terkait keamanan dan kerahasiaan data medis pasien. Data medis merupakan informasi yang sangat sensitif karena berkaitan langsung dengan kondisi kesehatan, identitas, serta riwayat penyakit seseorang. Oleh karena itu, muncul pertanyaan mendasar mengenai sejauh mana hak pasien atas keamanan dan kerahasiaan data medis terlindungi dalam praktik konsultasi kesehatan online.

Hak atas keamanan dan kerahasiaan data medis pasien pada prinsipnya merupakan bagian dari hak asasi manusia di bidang kesehatan. Hak tersebut dijamin dalam berbagai peraturan perundang-undangan di Indonesia, antara lain melalui pengaturan mengenai rekam medis, rahasia kedokteran, serta kewajiban tenaga kesehatan menjaga privasi pasien. Selain itu, etika profesi kedokteran secara tegas mewajibkan dokter untuk merahasiakan segala informasi yang diperoleh dalam hubungan terapeutik. Dalam konteks layanan kesehatan digital, kewajiban ini tetap melekat meskipun media pelayanan mengalami perubahan.¹

Dalam praktik konsultasi kesehatan online, perlindungan data medis sangat bergantung pada sistem teknologi yang digunakan oleh penyedia layanan. Platform kesehatan digital umumnya mengandalkan basis data berbasis website atau aplikasi yang terhubung dengan jaringan internet. Kondisi ini berbeda dengan sistem informasi rumah sakit konvensional yang bersifat tertutup dan hanya dapat diakses melalui jaringan internal. Sistem berbasis internet memiliki tingkat keterbukaan yang lebih tinggi dan berpotensi menjadi sasaran serangan siber. Akibatnya, risiko kebocoran, penyalahgunaan, atau akses tidak sah terhadap data medis pasien menjadi semakin besar.

Kerentanan keamanan data dalam layanan konsultasi online dapat terjadi dalam berbagai bentuk.² Contohnya adalah kebocoran data akibat lemahnya sistem enkripsi, penggunaan server pihak ketiga tanpa standar keamanan yang memadai, atau kesalahan pengelolaan hak akses pengguna. Selain itu, praktik penyimpanan data medis di cloud yang tidak seluruhnya berada di wilayah hukum Indonesia juga menimbulkan persoalan yurisdiksi hukum. Dalam kondisi demikian, pasien sering kali tidak mengetahui di mana dan bagaimana data medis mereka disimpan. Hal ini menunjukkan adanya ketimpangan informasi antara pasien dan penyedia layanan kesehatan online.

Di Indonesia, layanan konsultasi kesehatan online berkembang pesat seiring meningkatnya penggunaan telepon pintar dan internet. Layanan ini tidak hanya berdiri sendiri, tetapi sering kali terintegrasi dengan layanan kesehatan konvensional, seperti konsultasi lanjutan secara tatap muka.³ Dalam beberapa platform, dokter juga memberikan resep obat setelah konsultasi dilakukan melalui fitur chat atau video call. Praktik ini menimbulkan kekhawatiran terkait kualitas pelayanan medis, termasuk potensi kesalahan diagnosis dan terapi. Di sisi lain, proses tersebut juga melibatkan pertukaran data medis pasien secara intensif dalam ruang digital.

rapikan

Risiko dalam konsultasi kesehatan online tidak hanya berkaitan dengan aspek klinis, tetapi juga dengan aspek hukum dan etika. Ketidakjelasan identitas tenaga medis, lemahnya verifikasi kompetensi dokter, serta absennya kontrak terapeutik yang tegas dapat merugikan pasien.⁴ Fenomena penyalahgunaan identitas tenaga kesehatan atau praktik “dokteroid” menjadi

¹ Ikatan Dokter Indonesia. (2012). Kode etik kedokteran Indonesia.

² Kichloo, A., Albosta, M., Dettloff, K., Wani, F., El-Amir, Z., Singh, J., Aljadah, M., Chakinala, R. C., Kanugula, A. K., Solanki, S., & Chugh, S. (2020). Telemedicine, the current COVID-19 pandemic and the future: a narrative review and perspectives moving forward in the USA. *Family Medicine and Community Health*, 8(3), 1–9. <https://doi.org/10.1136/fmch-2020-000530>

³ Karl Fritz Pasaribu, Dedy Arisjulyanto, B. T. H. (2017). Pengembangan telemedicine dalam mengatasi konektivitas dan aksesibilitas pelayanan kesehatan. *Berita Kedokteran Masyarakat (BKM Public Health and Community Medicine)*, 2010(2015), 4258.

⁴ Karo Karo, R., & Pasaribu, D. (2019). Aspek Hukum Konsultasi Dokter Melalui Media Online di Indonesia. *Tadakulo Master Law Journal*, 3(2), 89–112.

tantangan serius dalam layanan kesehatan digital. Dalam situasi ini, data medis pasien berpotensi diakses oleh pihak yang tidak berwenang. Kondisi tersebut semakin mempertegas pentingnya sistem keamanan data yang kuat dan pengawasan yang efektif.

Teknologi digital pada dasarnya bersifat netral, namun penggunaannya dapat membawa dampak positif maupun negatif. Dalam konteks konsultasi kesehatan online, teknologi berperan sebagai alat yang mempermudah akses pelayanan kesehatan, tetapi juga dapat menjadi sumber risiko hukum. Pola interaksi berbasis web interaktif memungkinkan pertukaran data secara cepat, tetapi sekaligus membuka peluang manipulasi dan kebocoran informasi. Tanpa pengaturan yang memadai, pasien berada dalam posisi rentan terhadap pelanggaran privasi. Oleh karena itu, penggunaan teknologi dalam layanan kesehatan harus diiringi dengan prinsip kehati-hatian dan perlindungan hukum yang memadai.

Hingga saat ini, pengaturan mengenai konsultasi kesehatan online di Indonesia masih bersifat parsial dan tersebar dalam berbagai regulasi. Belum terdapat aturan khusus yang secara komprehensif mengatur standar keamanan sistem digital, pengelolaan data medis, serta tanggung jawab hukum platform kesehatan online. Kekosongan hukum ini berpotensi menimbulkan ketidakpastian bagi pasien ketika terjadi pelanggaran data medis. Selain itu, mekanisme penyelesaian sengketa akibat kebocoran data medis dalam layanan online juga belum diatur secara jelas. Kondisi ini menunjukkan perlunya penguatan regulasi yang adaptif terhadap perkembangan teknologi.

Selain aspek regulasi, kesadaran pasien terhadap hak atas keamanan dan kerahasiaan data medis juga masih relatif rendah. Banyak pasien menyetujui penggunaan layanan konsultasi online tanpa memahami secara utuh ketentuan informed consent dan kebijakan privasi platform. Persetujuan sering kali diberikan secara otomatis tanpa membaca risiko yang mungkin timbul. Akibatnya, pasien tidak memiliki posisi tawar yang kuat ketika terjadi pelanggaran data.⁵ Edukasi hukum kepada masyarakat menjadi faktor penting dalam memperkuat perlindungan hak pasien.

Berdasarkan uraian tersebut, dapat disimpulkan bahwa hak atas keamanan dan kerahasiaan data medis pasien dalam konsultasi kesehatan online merupakan isu hukum yang harus segera diungkapkan. Perkembangan layanan kesehatan digital harus diimbangi dengan regulasi yang komprehensif, sistem keamanan teknologi yang andal, serta penegakan etika profesi tenaga kesehatan. Tanpa perlindungan hukum yang memadai, kemajuan teknologi justru dapat merugikan pasien sebagai pihak yang paling rentan. Oleh karena itu, kajian ini menjadi penting untuk menganalisis perlindungan hukum terhadap keamanan dan kerahasiaan data medis pasien dalam praktik konsultasi kesehatan online di Indonesia.

Penelitian ini dimaksudkan untuk mengetahui bagaimana pengaturan dan pelaksanaan perlindungan hukum terhadap hak atas keamanan dan kerahasiaan data medis pasien dalam layanan konsultasi kesehatan online, mengidentifikasi berbagai permasalahan hukum yang dihadapi dalam penerapannya, serta menggambarkan upaya-upaya hukum dan kebijakan yang telah dan perlu dilakukan oleh negara, tenaga kesehatan, dan penyedia platform layanan kesehatan digital guna menjamin perlindungan data medis pasien secara efektif dan berkelanjutan.

⁵ Uscher-Pines, L., Mulcahy, A., Cowling, D., Hunter, G., Burns, R., & Mehrotra, A. (2016). Access and quality of care in direct-to-consumer telemedicine. *Telemedicine and E-Health*, 22(4), 282–287. <https://doi.org/10.1089/tmj.2015.0079>

METODE PENELITIAN

Penelitian ini menggunakan pendekatan hukum normatif, yaitu penelitian yang berfokus pada kajian terhadap norma, asas, dan sistem hukum yang mengatur hak atas keamanan dan kerahasiaan data medis pasien dalam layanan konsultasi kesehatan online.⁶ Pendekatan ini dipilih karena permasalahan yang dikaji berkaitan langsung dengan pengaturan hukum positif, prinsip perlindungan hak pasien, serta kewajiban hukum tenaga kesehatan dan penyedia platform layanan kesehatan digital. Penelitian hukum normatif bertujuan untuk menemukan preskripsi hukum yang seharusnya diterapkan dalam menjamin perlindungan data medis pasien. Dengan demikian, penelitian ini tidak menitikberatkan pada pengumpulan data empiris, melainkan pada analisis mendalam terhadap konstruksi norma hukum yang berlaku.

Jenis data yang digunakan dalam penelitian ini adalah data sekunder yang diperoleh melalui penelusuran bahan pustaka. Data sekunder tersebut terdiri atas tiga jenis bahan hukum, yaitu bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer merupakan sumber utama yang memiliki kekuatan mengikat, meliputi peraturan perundang-undangan yang relevan dengan perlindungan data medis dan layanan kesehatan, yurisprudensi yang berkaitan dengan sengketa kesehatan dan pelanggaran privasi, serta instrumen atau traktat internasional yang mengatur hak atas privasi dan perlindungan data. Bahan hukum primer ini menjadi dasar utama dalam melakukan analisis normatif.⁷

HASIL DAN PEMBAHASAN

Pengaturan dan Pelaksanaan Perlindungan Hukum Terhadap Hak Atas Keamanan dan Kerahasiaan Rekam Medis

Perlindungan atas keamanan dan kerahasiaan data medis pasien dalam layanan konsultasi kesehatan online merupakan bagian dari hak asasi manusia yang bersifat fundamental. Hak ini berkaitan dengan hak setiap orang untuk memperoleh perlindungan terhadap data pribadi yang melekat pada dirinya, termasuk hak atas pembelaan dan pemulihan apabila terjadi pelanggaran.⁸ Data medis pasien tidak hanya mencakup informasi klinis, tetapi juga data pribadi yang dapat mengidentifikasi individu, seperti nama, alamat, nomor telepon, data demografi, hingga alamat IP. Oleh karena itu, perlindungan data medis dalam layanan kesehatan digital tidak dapat dilepaskan dari rezim perlindungan data pribadi secara umum. Negara memiliki kewajiban untuk menjamin agar pemanfaatan teknologi dalam pelayanan kesehatan tetap menghormati dan melindungi hak-hak dasar pasien.

Perlindungan hukum dalam konteks ini merupakan upaya yang dilakukan oleh negara melalui pembentukan dan penegakan peraturan perundang-undangan untuk melindungi hak asasi manusia yang berpotensi dirugikan oleh pihak lain. Perlindungan hukum diberikan agar masyarakat memiliki kepastian dan rasa aman dalam memanfaatkan layanan kesehatan, termasuk layanan berbasis digital.⁹ Tanpa adanya perlindungan hukum yang jelas, kehidupan

⁶ Wiwik IA, Widiarty S. Buku Ajar: Metode Penelitian Hukum. Publika; 2024

⁷ Peter Mahmud Marzuki. Penelitian Hukum. 4th ed. Jakarta: Kencana; 2008.

⁸ Ramdoni, M. M., & Herdiansyah, M. I. (2023). Pengembangan sistem informasi konsultasi dokter menggunakan framework Laravel. *Journal of Information System Research (JOSH)*, 4(3), 831–839. <https://doi.org/10.47065/josh.v4i3.3276>

⁹ Kustiyanti, S. A. (2023). Smart hospital: Konsep, implementasi, dan tantangan. Dalam *Transformasi Rumah Sakit*

bermasyarakat dapat berjalan tanpa pedoman, sehingga membuka peluang terjadinya penyalahgunaan wewenang dan pelanggaran hak. Dalam layanan konsultasi kesehatan online, perlindungan hukum menjadi semakin penting karena relasi antara pasien, dokter, dan penyedia platform berlangsung dalam ruang digital yang memiliki risiko tinggi terhadap kebocoran data. Dengan demikian, hukum berfungsi sebagai instrumen pengendali sekaligus pelindung bagi kepentingan pasien.

Bentuk perlindungan hukum terhadap kerahasiaan data rekam medis pasien dalam layanan kesehatan online dapat diwujudkan melalui penerapan ketentuan peraturan perundang-undangan yang mengatur perlindungan data pribadi dan rahasia kedokteran. Perlindungan ini berangkat dari pengakuan bahwa hak atas perlindungan diri pribadi merupakan hak konstitusional setiap warga negara. Dalam praktik konsultasi kesehatan online, perlindungan tersebut menuntut adanya sistem pengamanan data yang memadai, seperti pembatasan akses, pengendalian otorisasi pengguna, dan pengelolaan data yang bertanggung jawab. Selain itu, penyelenggara layanan wajib memastikan bahwa data medis pasien tidak digunakan di luar tujuan pelayanan kesehatan. Kegagalan dalam melindungi data medis tidak hanya berimplikasi teknis, tetapi juga menimbulkan konsekuensi hukum dan etika.

Pelaksanaan perlindungan data medis pasien dalam layanan konsultasi kesehatan online bertumpu pada konsep pembagian kewajiban dan hak yang jelas dan terukur antara berbagai pihak yang terlibat. Dalam ekosistem konsultasi kesehatan online, terdapat minimal tiga aktor utama yang saling berinteraksi: (1) penyedia layanan kesehatan (dokter, fasilitas kesehatan), (2) penyedia platform digital (operator layanan konsultasi kesehatan online), dan (3) pasien sebagai pemilik data. Masing-masing memiliki peran dan tanggung jawab yang berbeda namun saling melengkapi.

1. Kewajiban Penyedia Layanan Kesehatan

Penyedia layanan kesehatan memiliki kewajiban fundamental untuk menjamin keamanan dan kerahasiaan data medis pasien.¹⁰ Kewajiban ini mencakup:

- **Keamanan Teknis Sistem:** Penyedia layanan wajib menerapkan teknologi keamanan informasi yang canggih dan proporsional dengan tingkat sensitifitas data yang dikelola. Teknologi enkripsi end-to-end (E2EE) merupakan standar minimum yang harus diterapkan untuk melindungi data medis dari akses tidak sah. Selain enkripsi, penyedia layanan juga harus menerapkan pengendalian akses yang ketat (access control) dengan sistem autentikasi multi-faktor untuk memastikan hanya pihak yang berwenang yang dapat mengakses data medis.
- **Privacy by Design:** Prinsip ini mengharuskan penyedia layanan untuk mengintegrasikan perlindungan data sejak tahap awal pengembangan dan perancangan platform digital. Bukan sesuatu yang ditambahkan kemudian, tetapi menjadi DNA dari sistem itu sendiri. Implikasinya adalah bahwa setiap fitur, algoritma, dan proses pemrosesan data harus dirancang dengan mempertimbangkan keamanan dan privasi pengguna. Sebagai contoh, penyedia platform harus membuat keputusan desain untuk meminimalkan pengumpulan data (data minimization), membatasi retensi data (limited data retention), dan memberikan kontrol penuh kepada pengguna atas datanya.

Indonesia Menuju Era Masyarakat 5.0 (hlm. 161).

¹⁰ Arif, M. A. I. (2018). Tinjauan hukum atas layanan medis berbasis online (Skripsi). Fakultas Hukum, Universitas Hasanuddin, Makassar.

- **Transparansi dan Informed Consent:** Penyedia layanan harus memberikan informasi yang jelas, mudah dipahami, dan tidak menyesatkan kepada pasien mengenai: (a) jenis data apa yang akan dikumpulkan; (b) untuk tujuan apa data tersebut digunakan; (c) bagaimana data disimpan dan dilindungi; (d) risiko dan potensi kebocoran data; (e) siapa pihak ketiga yang akan menerima akses ke data; dan (f) berapa lama data akan disimpan. Informasi ini harus diberikan sebelum pasien memberikan persetujuan (informed consent) secara sukarela, terinformasi, dan spesifik.
- **Pengawasan dan Monitoring Berkelanjutan:** Penyedia layanan harus melakukan pengawasan aktif terhadap seluruh proses pemrosesan data—mulai dari pengumpulan, penyimpanan, penggunaan, hingga penghapusan. Monitoring ini mencakup pencatatan akses (access logs), deteksi anomali (anomaly detection), dan audit berkala untuk memastikan kepatuhan terhadap kebijakan internal dan peraturan hukum.

2. Kewajiban Penyedia Platform Digital

Penyedia platform digital dalam konteks konsultasi kesehatan online memegang peranan khusus sebagai operator infrastruktur yang memfasilitasi interaksi antara pasien dan dokter.¹¹ Kewajiban penyedia platform mencakup:

- **Keamanan Infrastruktur:** Penyedia platform harus menjamin bahwa infrastruktur teknologi informasi mereka memiliki standar keamanan tinggi. Ini termasuk pemilihan data center yang tersertifikasi, implementasi redundansi sistem (backup dan disaster recovery), sertifikasi keamanan internasional seperti ISO 27001, dan compliance terhadap standar industri kesehatan seperti HIPAA (di yurisdiksi AS) atau standar lokal yang setara.
- **Pembatasan Akses dan Segregasi Data:** Penyedia platform harus membatasi akses mereka terhadap data medis pasien hanya sebatas yang diperlukan untuk kepentingan operasional teknis. Mereka tidak seharusnya memiliki akses penuh atau tidak terbatas terhadap konten data medis. Sebagaimana prinsip "need-to-know basis," hanya personel teknis yang bertanggung jawab atas operasional sistem yang berhak mengakses data, dan pun demikian akses mereka harus dicatat dan diaudit.
- **Perjanjian Pemrosesan Data (Data Processing Agreement):** Penyedia platform harus menjalin perjanjian tertulis yang jelas dengan penyedia layanan kesehatan mengenai bagaimana mereka memproses data medis. Perjanjian ini harus menguraikan secara rinci tanggung jawab masing-masing pihak, standar keamanan yang harus dipenuhi, mekanisme notifikasi apabila terjadi pelanggaran, dan hak-hak pasien yang harus dipenuhi.

3. Hak-Hak Pasien

Pasien sebagai subjek data memiliki hak-hak fundamental yang harus dilindungi dan dihormati:¹²

- **Hak atas Privasi dan Kerahasiaan:** Hak atas privasi dan kerahasiaan data medis merupakan hak asasi manusia yang telah lama diakui dalam berbagai instrumen hukum internasional dan nasional. Dalam konteks layanan kesehatan, hak ini berarti pasien berhak untuk memiliki

¹¹ Muhammad, S., Sosiawaty, I., Julia, P., & Patty, T. (2023). Analisis kinerja pelayanan kesehatan tenaga medis di Puskesmas Air Besar Negeri Batu Merah Kecamatan Sirimau Kota Ambon Provinsi Maluku. *Jurnal PROFESI*, 10(1), 197–210. <https://jurnal.unived.ac.id/index.php/prof/article/view/3740>

¹² Fariz, M. R. (2021). Pola komunikasi dokter pada pasien melalui aplikasi Halodoc (Skripsi). Fakultas Dakwah dan Komunikasi, UIN Ar-Raniri, Banda Aceh.

kendali penuh atas informasi medisnya dan memastikan bahwa informasi tersebut tidak diungkapkan kepada pihak yang tidak berhak tanpa persetujuannya.

- Hak untuk Mengetahui dan Mengakses Data: Pasien memiliki hak untuk mengetahui informasi apa yang telah dikumpulkan tentang dirinya, bagaimana data tersebut digunakan, dan dengan siapa data tersebut dibagikan. Hak ini mewujudkan prinsip transparansi dan akuntabilitas dari penyedia layanan. Pasien juga berhak untuk mengakses data medisnya secara lengkap dan dalam format yang mudah dipahami.
- Hak untuk Merekifikasi dan Menghapus Data: Jika data medis yang disimpan tidak akurat, pasien memiliki hak untuk meminta koreksi. Demikian pula, pasien memiliki hak untuk meminta penghapusan data medisnya setelah tidak lagi diperlukan untuk tujuan awal pengumpulan, dengan tetap mempertimbangkan kewajiban retensi data untuk kepentingan medis atau hukum.
- Hak untuk Memberikan atau Mencabut Persetujuan: Persetujuan pasien tidak boleh dianggap sebagai sesuatu yang bersifat permanen dan tidak dapat diubah. Pasien harus memiliki kebebasan untuk memberikan atau mencabut persetujuan mereka kapan saja, tanpa penalti atau hambatan yang tidak wajar.

Identifikasi Berbagai Permasalahan Hukum yang Dihadapi Dalam Penerapannya

Meskipun kerangka normatif perlindungan data medis pasien telah diatur dalam berbagai peraturan perundang-undangan, pelaksanaan perlindungan hukum dalam layanan konsultasi kesehatan online masih menghadapi beragam permasalahan hukum. Tantangan tersebut meliputi aspek regulasi yang belum adaptif, legalitas tenaga medis, batasan kewenangan praktik online, serta lemahnya sistem pengamanan data. Perkembangan teknologi kesehatan yang sangat cepat sering kali tidak diimbangi dengan pembaruan regulasi yang memadai. Akibatnya, muncul celah hukum yang berpotensi merugikan pasien sebagai pemilik data medis. Kondisi ini menunjukkan bahwa perlindungan hukum dalam layanan kesehatan digital belum sepenuhnya efektif.

Permasalahan utama yang dihadapi adalah kesenjangan regulasi dan implementasi hukum. Regulasi yang ada, seperti Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Perlindungan Data Pribadi, belum sepenuhnya dirancang secara spesifik untuk mengatur kompleksitas layanan kesehatan online. Peran penyedia platform digital sebagai pihak ketiga yang mengelola data medis pasien belum diatur secara rinci, terutama terkait pembagian tanggung jawab hukum apabila terjadi kebocoran data. Selain itu, terdapat potensi tumpang tindih dan celah pengaturan antara regulasi kesehatan, teknologi informasi, dan perlindungan data pribadi. Ketidakharmonisan regulasi ini menyulitkan penegakan hukum secara efektif.

Risiko keamanan siber dan pelanggaran privasi menjadi permasalahan hukum yang sangat menonjol dalam layanan konsultasi kesehatan online. Data medis pasien merupakan data yang sangat sensitif dan bernilai tinggi sehingga menjadi target utama kejahatan siber. Ancaman kebocoran, peretasan, dan penyalahgunaan data dapat terjadi akibat lemahnya sistem keamanan digital yang digunakan oleh penyedia layanan. Penyalahgunaan data medis tidak hanya menimbulkan kerugian materiil, tetapi juga kerugian immateriil berupa pencemaran nama baik, pelanggaran kehormatan, dan tekanan psikologis bagi pasien. Dalam konteks ini, perlindungan hukum terhadap privasi pasien sering kali belum memberikan rasa aman yang optimal.

Berbagai kasus kebocoran data kesehatan di Indonesia menunjukkan lemahnya sistem

perlindungan data medis dalam praktik.¹³ Pada awal tahun 2022, publik dihebohkan dengan kebocoran data kesehatan pasien yang berasal dari server milik Kementerian Kesehatan, dengan ukuran data mencapai ratusan gigabita dan mencakup jutaan informasi pasien. Sebelumnya, pada tahun 2020, ratusan ribu data pasien COVID-19 dilaporkan diperjualbelikan di forum daring. Pada tahun 2021, jutaan data pengguna aplikasi e-HAC juga mengalami kebocoran akibat peretasan. Kasus-kasus tersebut memperlihatkan bahwa bahkan sistem yang dikelola oleh institusi negara pun belum sepenuhnya aman dari serangan siber.

Selain faktor teknis, penyalahgunaan data pribadi juga menjadi persoalan hukum.¹⁴ Data medis seperti hasil laboratorium, foto pemeriksaan, dan riwayat penyakit memiliki nilai ekonomi dan dapat disalahgunakan untuk kepentingan komersial maupun kejahatan siber. Penyalahgunaan ini dapat terjadi baik oleh pihak eksternal maupun internal yang memiliki akses terhadap sistem. Dalam layanan kesehatan online, data sering kali dikelola oleh pihak ketiga, seperti penyedia cloud atau pengembang aplikasi, yang belum tentu berada dalam pengawasan ketat otoritas kesehatan. Kompleksitas rantai pengelolaan data ini meningkatkan risiko pelanggaran hak pasien.

Permasalahan hukum lainnya berkaitan dengan tantangan sumber daya manusia dan rendahnya kesadaran hukum. Literasi digital pasien dan tenaga kesehatan masih relatif rendah, terutama terkait risiko keamanan data dan perlindungan privasi. Banyak pasien memberikan persetujuan penggunaan data tanpa memahami sepenuhnya implikasi hukum dan teknisnya. Di sisi lain, tenaga kesehatan dan pengelola fasilitas layanan kesehatan belum seluruhnya memiliki kompetensi yang memadai dalam mengelola sistem rekam medis elektronik dan keamanan data. Keterbatasan pemahaman ini berpotensi menyebabkan kelalaian yang berdampak pada kebocoran atau penyalahgunaan data medis pasien.

Permasalahan penegakan hukum dan sanksi juga menjadi faktor yang memperlemah perlindungan data medis pasien.¹⁵ Meskipun ketentuan sanksi telah diatur dalam berbagai peraturan perundang-undangan, implementasinya masih belum optimal. Proses pembuktian pelanggaran data digital sering kali kompleks dan membutuhkan keahlian teknis khusus. Selain itu, belum adanya mekanisme pengaduan yang mudah diakses dan responsif membuat pasien enggan melaporkan pelanggaran yang dialaminya. Akibatnya, efek jera terhadap pelaku pelanggaran perlindungan data medis menjadi lemah.

Upaya-Upaya Hukum dan Kebijakan dalam Menjaga Keamanan dan Kerahasiaan Pasien

Upaya perlindungan hukum terhadap keamanan dan kerahasiaan data medis pasien dalam layanan konsultasi kesehatan online di Indonesia pada dasarnya telah memiliki landasan normatif yang cukup kuat. Berikut uraiannya:

1. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan instrumen hukum utama yang menjadi rujukan dalam perlindungan data medis pasien dalam layanan konsultasi kesehatan online di Indonesia. Undang-undang ini secara eksplisit mengklasifikasikan data pribadi ke dalam dua kategori, yaitu data pribadi yang

¹³ Mangesti, Y. A. (2021). Perlindungan hukum data pribadi pasien telemedicine. Kompasiana. Diakses pada 1 Oktober 2025 dari <https://www.kompasiana.com>

¹⁴ Jusuf, E. C., Kumala, R., & Adriano, A. (2023). Tinjauan hukum kerahasiaan rekam medis dalam laporan kesehatan ibu dan anak berbasis digital. *Wajah Hukum*, 7(1), 28.

¹⁵ K. F., Amalia, dkk. (2022). Scoping review: Hambatan penerapan telemedicine di Indonesia. *Bandung Conference Series: Medical Science*, 2(1).

bersifat umum dan data pribadi yang bersifat spesifik sebagaimana diatur dalam Pasal 4. Data kesehatan, termasuk rekam medis, secara tegas dikategorikan sebagai data pribadi yang bersifat spesifik sebagaimana disebutkan dalam Pasal 4 ayat (2) huruf a, sehingga memperoleh tingkat perlindungan hukum yang lebih tinggi. Konsekuensinya, setiap pemrosesan data medis pasien dalam layanan konsultasi kesehatan online harus memenuhi standar perlindungan yang ketat dan tidak dapat diperlakukan sama dengan data pribadi biasa. Dengan pengaturan ini, negara menempatkan data medis pasien sebagai objek perlindungan hukum yang prioritas karena sifatnya yang sensitif dan berdampak langsung pada martabat serta privasi individu.

Lebih lanjut, Pasal 35 sampai dengan Pasal 39 UU PDP mengatur secara komprehensif kewajiban pengendali data pribadi, yang dalam konteks konsultasi kesehatan online adalah fasilitas pelayanan kesehatan dan penyedia aplikasi layanan kesehatan online. Pengendali data diwajibkan untuk melindungi dan memastikan keamanan data pribadi melalui penerapan langkah-langkah teknis dan operasional yang memadai, dengan memperhatikan tingkat risiko dari data yang diproses. Pasal 36 secara khusus menegaskan kewajiban pengendali data untuk menjaga kerahasiaan data pribadi dalam setiap tahapan pemrosesan. Dalam praktik konsultasi kesehatan online, kewajiban ini berlaku sejak pasien memberikan *informed consent* dan menyerahkan data medisnya dalam bentuk rekam medis elektronik. Rekam medis elektronik tersebut wajib dijaga kerahasiaannya dan tidak boleh diakses, digunakan, atau diungkapkan di luar tujuan pelayanan kesehatan.

Sebagai bentuk perlindungan hukum preventif, Pasal 39 UU PDP mewajibkan pengendali data untuk melakukan upaya pencegahan melalui penggunaan sistem keamanan yang andal, aman, dan bertanggung jawab sesuai dengan ketentuan peraturan perundang-undangan. Kewajiban ini menuntut penyedia layanan konsultasi kesehatan online untuk memiliki kebijakan internal dan sistem pengamanan data yang sejalan dengan standar perlindungan data pribadi. Dengan demikian, perlindungan data medis pasien tidak hanya berhenti pada norma hukum, tetapi harus diwujudkan dalam tata kelola sistem, kebijakan aplikasi, serta pengawasan terhadap seluruh pihak yang terlibat dalam pemrosesan data. Prinsip perlindungan ini menegaskan bahwa hak pasien atas kerahasiaan data medis merupakan bagian dari hak konstitusional atas perlindungan diri pribadi.

2. Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan

Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan menjadi landasan hukum sektoral yang memperkuat perlindungan hak pasien, termasuk hak atas keamanan dan kerahasiaan data medis dalam layanan konsultasi kesehatan online. Undang-undang ini menegaskan bahwa setiap orang berhak memperoleh pelayanan kesehatan yang bermutu, aman, dan bertanggung jawab, tanpa diskriminasi dan dengan menjunjung tinggi martabat kemanusiaan. Hak atas informasi kesehatan dan perlindungan terhadap data medis diposisikan sebagai bagian integral dari hak kesehatan itu sendiri. Dengan demikian, perlindungan data medis pasien tidak dapat dipisahkan dari kewajiban negara untuk menjamin mutu dan keselamatan pelayanan kesehatan, termasuk pelayanan yang diselenggarakan melalui media digital atau konsultasi kesehatan online.

Lebih lanjut, Undang-Undang Kesehatan menempatkan kerahasiaan data medis sebagai bagian dari kewajiban penyelenggara pelayanan kesehatan dan tenaga kesehatan dalam menjalankan praktik profesionalnya. Setiap fasilitas pelayanan kesehatan dan tenaga medis wajib menjaga kerahasiaan informasi kesehatan pasien yang diperoleh dalam hubungan terapeutik. Kewajiban

ini berlaku tanpa membedakan bentuk pelayanan, baik pelayanan kesehatan konvensional maupun pelayanan kesehatan berbasis teknologi informasi. Dalam konteks konsultasi kesehatan online, pengelolaan rekam medis elektronik harus dilakukan dengan prinsip kehati-hatian dan tanggung jawab profesional yang sama seperti rekam medis konvensional. Pelanggaran terhadap kewajiban ini dapat dianggap sebagai pelanggaran hak pasien sekaligus pelanggaran terhadap standar pelayanan kesehatan.

Undang-Undang Nomor 17 Tahun 2023 juga menegaskan bahwa pelayanan kesehatan yang bermutu dan bertanggung jawab mensyaratkan adanya legalitas yang jelas serta pengawasan oleh negara. Fasilitas pelayanan kesehatan dan tenaga kesehatan yang menyelenggarakan layanan konsultasi online wajib memenuhi persyaratan perizinan, standar kompetensi, dan standar operasional yang ditetapkan. Pelayanan kesehatan yang tidak memenuhi persyaratan tersebut tidak hanya berpotensi menurunkan mutu pelayanan, tetapi juga meningkatkan risiko pelanggaran keamanan dan kerahasiaan data medis pasien. Oleh karena itu, penguatan pengawasan dan pembinaan oleh pemerintah menjadi bagian penting dalam menjamin perlindungan hukum bagi pasien.

3. Undang-Undang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan atas Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik disusun dengan tujuan menjaga ruang digital Indonesia yang bersih, sehat, beretika, produktif, dan berkeadilan, sekaligus memberikan kepastian hukum serta melindungi kepentingan umum. Undang-undang ini memperluas dan mempertegas kewajiban penyelenggara sistem elektronik dalam penyelenggaraan layanan berbasis digital, termasuk layanan kesehatan online atau konsultasi kesehatan online. Penambahan sejumlah pasal baru, antara lain Pasal 13A, Pasal 16A, Pasal 16B, Pasal 18A, Pasal 27A dan B, serta Pasal 40A, menunjukkan adanya upaya negara untuk menyesuaikan hukum dengan perkembangan teknologi informasi yang semakin kompleks. Salah satu ketentuan penting adalah Pasal 13A yang secara tegas mengatur jenis layanan yang dapat diselenggarakan oleh penyelenggara sistem elektronik.

Dalam Pasal 13A UU ITE ditegaskan bahwa:

1. *“Setiap penyelenggara sistem elektronik atau sistem online wajib menyelenggarakan sistem online secara andal dan aman serta bertanggung jawab atas kelancaran operasional sistem elektronik.”*
2. *“Penyelenggara sistem elektronik bertanggung jawab atas penyelenggaraan sistem elektronik.”*
3. *“Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku sepanjang dapat dibuktikan adanya keadaan memaksa, kesalahan dan/atau kelalaian pengguna sistem elektronik.”*

Ketentuan ini menempatkan penyelenggara sistem elektronik, termasuk platform layanan kesehatan digital, sebagai subjek hukum yang memiliki tanggung jawab penuh atas keamanan dan keandalan sistem yang dikelolanya. Dalam konteks konsultasi kesehatan online, kewajiban tersebut mencakup perlindungan terhadap data medis pasien yang diproses melalui sistem elektronik.

Namun demikian, dalam praktik penyelenggaraan pelayanan kesehatan berbasis digital,

perlindungan hukum terhadap data pasien masih menghadapi tantangan normatif. Pasal 15 UU ITE yang mengatur tanggung jawab pengamanan data oleh penyelenggara sistem elektronik masih dipandang sebagai norma samar (*vage normen*) karena belum memberikan batasan teknis yang jelas, khususnya dalam konteks layanan konsultasi kesehatan online. Di sisi lain, Peraturan Menteri Kesehatan Nomor 20 Tahun 2019 tentang Konsultasi kesehatan online masih berfokus pada hubungan pelayanan antara dokter dan pasien, dan belum mengatur secara rinci mengenai tanggung jawab penyelenggara platform serta perlindungan hukum terhadap data pribadi dan rekam medis pasien. Kondisi ini menimbulkan celah hukum yang berpotensi melemahkan perlindungan data medis pasien.

Perlindungan data pribadi dalam UU ITE ditegaskan melalui ketentuan Pasal 26. Pasal 26 ayat (1) menyatakan bahwa *“Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan.”* Selanjutnya, Pasal 26 ayat (2) menyebutkan bahwa *“Setiap orang yang melanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.”* Ketentuan ini memberikan dasar hukum bagi pasien sebagai pemilik data medis untuk menuntut ganti rugi apabila data pribadinya digunakan tanpa persetujuan.

Penjelasan Pasal 26 UU ITE menegaskan bahwa perlindungan data pribadi merupakan bagian dari hak pribadi (*privacy rights*). Hak pribadi tersebut mencakup hak untuk menikmati kehidupan pribadi dan bebas dari gangguan, hak untuk berkomunikasi tanpa dimata-matai, serta hak untuk mengawasi akses terhadap informasi dan data pribadi seseorang. Dalam konteks layanan konsultasi kesehatan online, data medis pasien merupakan bagian dari kehidupan pribadi yang paling sensitif. Oleh karena itu, setiap bentuk pengolahan, penyimpanan, dan distribusi data medis melalui sistem elektronik harus mendapatkan persetujuan eksplisit dari pasien dan dilakukan secara bertanggung jawab.

UU ITE juga memberikan dasar pengenaan sanksi pidana terhadap penyalahgunaan data elektronik, termasuk data medis pasien. Pasal 32 UU ITE mengatur larangan perbuatan mengubah, menambah, mengurangi, mentransmisikan, merusak, menghilangkan, memindahkan, atau membuka informasi elektronik yang bersifat rahasia tanpa hak. Apabila perbuatan tersebut mengakibatkan terbukanya informasi elektronik yang bersifat rahasia kepada publik, maka pelaku dapat dikenakan sanksi pidana. Ketentuan ini relevan dalam kasus kebocoran atau peretasan data medis pasien yang terjadi dalam layanan kesehatan online.

Lebih lanjut, Pasal 35 dan Pasal 51 ayat (1) UU ITE mengatur sanksi pidana bagi setiap orang yang dengan sengaja membuat informasi elektronik atau dokumen elektronik seolah-olah data yang otentik. Pasal 51 ayat (1) menyatakan bahwa *“Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).”* Ketentuan ini dapat diterapkan dalam konteks pemalsuan data medis elektronik yang berpotensi merugikan pasien maupun fasilitas pelayanan kesehatan. Selain itu, Pasal 48 UU ITE juga mengatur ancaman pidana terhadap pelanggaran Pasal 32 dengan pidana penjara dan denda yang bervariasi sesuai dengan tingkat pelanggaran.

Pembahasan

Secara konseptual, UU Perlindungan Data Pribadi, UU Kesehatan, dan UU ITE memiliki kesamaan mendasar dalam mengakui perlindungan data pribadi sebagai bagian dari hak

fundamental individu di era digital. Ketiganya menempatkan data kesehatan sebagai informasi yang sangat sensitif dan memerlukan perlindungan hukum yang lebih tinggi dibandingkan data pribadi biasa. UU PDP secara tegas mengklasifikasikan data kesehatan sebagai data pribadi khusus yang berisiko tinggi apabila disalahgunakan, sementara UU Kesehatan memperkuatnya dengan menempatkan kerahasiaan data medis sebagai bagian dari mutu dan keselamatan pelayanan kesehatan. UU ITE melengkapi kerangka tersebut dengan pengaturan mengenai perlindungan data pribadi dalam penyelenggaraan sistem elektronik, sehingga menciptakan perlindungan berlapis terhadap privasi pasien dalam layanan kesehatan berbasis digital.

Selain pengakuan terhadap sensitivitas data kesehatan, ketiga undang-undang tersebut juga memiliki kesamaan dalam prinsip dasar pemrosesan data pribadi, yakni adanya keharusan dasar hukum yang sah dan persetujuan dari subjek data. UU PDP mengatur secara komprehensif dasar-dasar hukum pemrosesan data, dengan persetujuan pasien (*informed consent*) sebagai landasan utama dalam layanan kesehatan. UU Kesehatan mensyaratkan persetujuan pasien dalam pengelolaan rekam medis dan melarang pengungkapan rahasia medis tanpa alasan yang dibenarkan hukum. UU ITE menegaskan larangan penggunaan dan pengungkapan data pribadi tanpa persetujuan pemilik data dalam transaksi elektronik. Kesamaan prinsip ini membentuk suatu *safety net* normatif yang saling melengkapi, sehingga perlindungan hukum terhadap data medis pasien tetap dapat ditegakkan meskipun salah satu instrumen hukum belum diterapkan secara optimal.

Perbedaan: Fokus, Cakupan, dan Tingkat Detail Pengaturan

Meskipun memiliki tujuan bersama, ketiga undang-undang tersebut memiliki perbedaan signifikan dalam fokus, cakupan, dan tingkat detail pengaturan yang mencerminkan filosofi dan domain masing-masing.

1. UU Perlindungan Data Pribadi: Pendekatan Berbasis Pengendali-Prosesor

UU Perlindungan Data Pribadi mengadopsi pendekatan berbasis pengendali dan prosesor data yang menekankan tata kelola data pribadi secara komprehensif dan berorientasi teknis-operasional. Pendekatan ini memiliki keunggulan karena mengatur kewajiban pengendali data secara rinci, seperti penerapan *privacy by design*, persetujuan yang eksplisit, pengelolaan akses, audit keamanan, serta kewajiban notifikasi apabila terjadi pelanggaran data. Selain itu, UU PDP bersifat fleksibel secara sektoral karena memberikan ruang bagi kementerian atau lembaga terkait, termasuk sektor kesehatan, untuk menetapkan standar perlindungan yang lebih spesifik sesuai karakteristik layanannya. Pembentukan Otoritas Jaminan Perlindungan Data Pribadi sebagai lembaga independen juga memperkuat pengawasan dan penegakan hukum terhadap pelanggaran perlindungan data pribadi.

Namun demikian, dalam konteks data medis dan layanan konsultasi kesehatan online, pendekatan UU PDP masih memiliki keterbatasan. UU ini belum secara eksplisit mengatur karakteristik khusus layanan kesehatan digital, seperti pembagian tanggung jawab hukum antara dokter, fasilitas pelayanan kesehatan, dan penyedia platform teknologi. Fokus utama UU PDP pada aspek teknis pengelolaan data juga belum sepenuhnya mengakomodasi dimensi hubungan terapeutik dokter-pasien yang sarat dengan nilai etika, kepercayaan, dan profesionalisme medis. Akibatnya, meskipun UU PDP memberikan kerangka perlindungan data yang kuat, penerapannya dalam layanan kesehatan online tetap memerlukan pengaturan sektoral yang lebih spesifik agar selaras dengan karakteristik dan kebutuhan praktik kedokteran.

2. UU Kesehatan: Pendekatan Berbasis Etika dan Tanggung Jawab Profesional

UU Kesehatan mengadopsi pendekatan berbasis etika dan tanggung jawab profesional dengan menempatkan perlindungan data medis sebagai bagian integral dari hubungan terapeutik antara pasien dan penyedia layanan kesehatan. Pendekatan ini bersifat holistik dan manusiawi karena memandang pasien bukan sekadar sebagai pemilik data, melainkan sebagai subjek hak atas kesehatan dan privasi yang harus dilindungi secara menyeluruh. UU Kesehatan juga mengaitkan kewajiban menjaga kerahasiaan data medis dengan standar etika profesi tenaga kesehatan, sehingga pelanggaran terhadap kerahasiaan dapat diproses melalui mekanisme disiplin profesi. Selain itu, undang-undang ini memberikan kepastian bahwa tanggung jawab atas perlindungan data medis berada pada penyelenggara pelayanan kesehatan, yang harus menjamin mutu, keselamatan, dan kerahasiaan dalam setiap bentuk pelayanan.

Namun demikian, pendekatan UU Kesehatan memiliki keterbatasan dalam menghadapi kompleksitas layanan kesehatan digital. Pengaturan mengenai keamanan data masih bersifat normatif dan belum merinci standar teknis seperti enkripsi, pengendalian akses, dan manajemen risiko sistem elektronik yang krusial dalam konsultasi kesehatan online. Selain itu, pengaturan rekam medis dalam UU Kesehatan lebih berorientasi pada layanan kesehatan konvensional dan belum sepenuhnya mengakomodasi karakteristik rekam medis elektronik yang dikelola oleh platform pihak ketiga. Dari sisi penegakan hukum, UU Kesehatan juga belum didukung oleh mekanisme pengawasan independen, sehingga perlindungan data medis pasien masih sangat bergantung pada disiplin profesi dan upaya hukum perdata, yang dalam praktiknya memiliki keterbatasan efektivitas.

UU Informasi dan Transaksi Elektronik mengadopsi pendekatan berbasis sistem elektronik dengan menempatkan penyelenggaraan teknologi informasi sebagai fokus utama pengaturan hukum di ruang digital. Sebagai undang-undang pilar dalam regulasi dunia digital di Indonesia, UU ITE mengatur berbagai aspek transaksi elektronik, komunikasi digital, dan pengelolaan sistem elektronik yang menjadi fondasi bagi layanan berbasis teknologi, termasuk layanan kesehatan online. Pendekatan ini menegaskan bahwa setiap penyelenggara sistem elektronik wajib menjaga keamanan, keandalan, dan kelangsungan operasional sistem yang dikelolanya. Dengan cakupan yang luas, UU ITE menjadi kerangka dasar dalam memastikan bahwa aktivitas digital berlangsung secara tertib dan bertanggung jawab.

Keunggulan utama UU ITE terletak pada kemampuannya menghubungkan perlindungan data dengan aspek keamanan siber dan pencegahan kejahatan digital. Pengaturan mengenai larangan peretasan, pengubahan, pemindahan, dan pembukaan informasi elektronik tanpa hak menunjukkan bahwa perlindungan data tidak hanya dipahami sebagai isu privasi, tetapi juga sebagai bagian dari upaya menjaga keamanan nasional dan kepentingan publik. Dalam konteks layanan kesehatan online, ketentuan ini relevan karena data medis pasien merupakan target potensial kejahatan siber. Kewajiban menjaga keamanan sistem elektronik memberikan dasar hukum bagi penindakan terhadap pelanggaran yang mengancam integritas dan kerahasiaan data medis.

Namun demikian, pendekatan UU ITE memiliki keterbatasan dalam memberikan perlindungan yang spesifik terhadap data medis pasien. Norma-norma mengenai keamanan sistem elektronik masih bersifat umum dan menggunakan istilah yang membuka ruang tafsir luas, sehingga berpotensi menimbulkan ketidakpastian hukum dalam praktik. Selain itu, UU ITE belum secara khusus membedakan karakteristik data medis sebagai data yang sangat sensitif dan

memerlukan standar perlindungan yang lebih ketat dibandingkan data elektronik lainnya. Fokus utama undang-undang ini juga lebih menitikberatkan pada keamanan infrastruktur sistem elektronik daripada perlindungan privasi dan kerahasiaan data, sehingga memerlukan harmonisasi dengan UU PDP dan UU Kesehatan agar perlindungan data medis pasien dalam layanan kesehatan digital dapat terwujud secara optimal.

Tabel 1. Komparasi UU PDP UU Kesehatan dan UU ITE

Aspek	UU PDP	UU Kesehatan	UU ITE
Fokus Utama	Tata kelola data pribadi (teknis & operasional)	Hak & tanggung jawab dalam pelayanan kesehatan	Penyelenggaraan sistem elektronik & cybercrime
Model Dasar	Pengendali-Prosesor	Hubungan Dokter-Pasien & Penyelenggara Pelayanan	Penyelenggara Sistem Elektronik
Kategori Data Medis	Data pribadi khusus (spesifik)	Data yang wajib dirahasiakan (dalam konteks medis)	Data pribadi dalam transaksi elektronik (umum)
Standar Teknis	Rinci (enkripsi, access control, audit log, dll)	Kurang spesifik untuk sistem digital	Umum (standar keamanan yang diperlukan)
Otoritas Pengawasan	OJPP (independen)	Dinas Kesehatan, Kemenkes	Kemenkominfo (melalui BRTI)
Sanksi	Pidana & administratif (denda, pencabutan izin)	Pidana, perdata, & disiplin profesi	Pidana & denda administratif
Mekanisme Penyelesaian	Gugatan ke OJPP, gugatan perdata, gugatan pidana	Gugatan perdata, gugatan pidana, disiplin profesi	Gugatan pidana, gugatan perdata
Kelebihan	Komprehensif teknis, ada otoritas independen	Humanis, berbasis etika profesi	Cakupan luas teknologi informasi
Kelemahan	Tidak spesifik konsultasi kesehatan online	Kurang detail teknis, belum mengatur RME pihak ketiga	Norma samar, belum spesifik data medis

Meskipun ketiga undang-undang memiliki fondasi yang sejalan, ketidaksinkronan dalam fokus, cakupan, dan tingkat detail pengaturan menciptakan celah-celah hukum yang signifikan. Celah-celah ini berpotensi mengurangi efektivitas perlindungan data medis pasien dalam layanan konsultasi kesehatan online dan menimbulkan ketidakpastian hukum.

Celah 1: Ketidakjelasan Standar Teknis Keamanan

Salah satu celah hukum utama dalam perlindungan data medis pasien pada layanan konsultasi kesehatan online adalah ketidakjelasan standar teknis keamanan yang bersifat seragam dan wajib bagi penyelenggara layanan. UU Perlindungan Data Pribadi mengamanatkan penerapan standar keamanan dan privasi, namun tidak secara rinci mendefinisikan bentuk dan parameter teknis standar tersebut. UU Kesehatan mewajibkan penyelenggara pelayanan kesehatan menjaga kerahasiaan data medis pasien, tetapi tidak memberikan panduan teknis mengenai bagaimana kewajiban tersebut harus diimplementasikan dalam sistem digital.

Sementara itu, UU ITE hanya menyebut kewajiban penerapan “standar keamanan yang diperlukan” tanpa spesifikasi teknis yang jelas, sehingga membuka ruang interpretasi yang luas.

Ketidakjelasan pengaturan ini berdampak langsung pada praktik penyelenggaraan layanan konsultasi kesehatan online. Penyedia layanan memiliki kebebasan yang sangat besar dalam menentukan tingkat keamanan sistem yang digunakan, mulai dari penerapan enkripsi dasar hingga penggunaan standar keamanan internasional yang lebih ketat. Akibatnya, terjadi perbedaan tingkat perlindungan data medis yang signifikan antarplatform, yang pada akhirnya dapat merugikan pasien sebagai pemilik data. Kondisi ini menunjukkan perlunya regulasi turunan yang lebih teknis dan operasional, idealnya disusun oleh Kementerian Kesehatan bekerja sama dengan kementerian terkait, untuk menetapkan standar minimum keamanan data medis. Standar tersebut perlu mencakup aspek enkripsi, pengendalian akses, pencatatan aktivitas (*audit log*), pemulihan bencana (*disaster recovery*), dan mekanisme keamanan lainnya guna menjamin perlindungan data medis pasien secara konsisten dan berkeadilan.

Celah 2: Pembagian Tanggung Jawab yang Tidak Jelas

rangkum menjadi 3 paragraf yang informative Isu Pokok: Belum terdapat pengaturan yang tegas mengenai pembagian tanggung jawab hukum antara dokter, fasilitas kesehatan, dan penyedia platform digital dalam hal perlindungan data medis. Manifestasi Celah: • UU PDP mengatur pengendali data dan prosesor data, tetapi dalam konteks konsultasi kesehatan online, tidak jelas apakah dokter adalah "pengendali data" atau "prosesor data"; apakah fasilitas kesehatan memiliki tanggung jawab bersama atau penuh; dan apakah penyedia platform adalah "prosesor data" atau "pihak ketiga yang menerima data." • UU Kesehatan menyatakan bahwa setiap penyelenggara pelayanan kesehatan bertanggung jawab, tetapi tidak jelas bagaimana tanggung jawab ini terbagi dalam ekosistem konsultasi kesehatan online. • UU ITE mengatur penyelenggara sistem elektronik, tetapi tidak jelas apakah ini mencakup penyedia platform konsultasi kesehatan online dan dalam hal apa tanggung jawab mereka. Dampak Praktis: Ketika terjadi kebocoran atau penyalahgunaan data medis, sulit untuk menentukan pihak mana yang paling bertanggung jawab dan harus memikul konsekuensi hukum. Situasi ini menciptakan "moral hazard" di mana masing-masing pihak dapat saling menyalahkan, sementara pasien tetap menjadi korban. Contoh konkret: jika data medis bocor karena sistem platform yang lemah, apakah dokter yang menggunakan platform bisa disalahkan? Apakah fasilitas kesehatan yang merekomendasikan platform bisa disalahkan? Atau hanya penyedia platform yang bertanggung jawab? Diperlukan: Peraturan pemerintah atau peraturan menteri yang secara tegas menguraikan pembagian tanggung jawab dalam layanan konsultasi kesehatan online, mencakup: (a) tanggung jawab dokter dalam memilih platform yang aman dan memberikan informed consent yang tepat; (b) tanggung jawab fasilitas kesehatan dalam mengawasi dan mengaudit implementasi konsultasi kesehatan online mereka; (c) tanggung jawab penyedia platform dalam menjaga keamanan infrastruktur dan data; dan (d) mekanisme koordinasi dan pertanggungjawaban bersama.

Salah satu persoalan krusial dalam perlindungan data medis pasien pada layanan konsultasi kesehatan online adalah belum adanya pengaturan yang tegas mengenai pembagian tanggung jawab hukum antara dokter, fasilitas pelayanan kesehatan, dan penyedia platform digital. UU Perlindungan Data Pribadi memang memperkenalkan konsep pengendali data dan prosesor data, namun dalam praktik konsultasi kesehatan online posisi masing-masing aktor belum jelas. Tidak terdapat kepastian apakah dokter berperan sebagai pengendali atau sekadar prosesor data, apakah fasilitas kesehatan memikul tanggung jawab penuh atau bersama, serta bagaimana status hukum penyedia platform digital dalam pengelolaan data medis pasien.

Ketidakjelasan ini menimbulkan kerancuan dalam penerapan tanggung jawab hukum.

UU Kesehatan dan UU ITE juga belum memberikan kejelasan pembagian peran tersebut. UU Kesehatan menyatakan bahwa penyelenggara pelayanan kesehatan bertanggung jawab atas pelayanan yang diberikan, namun tidak menguraikan bagaimana tanggung jawab tersebut dibagi dalam ekosistem konsultasi kesehatan online yang melibatkan pihak ketiga berbasis teknologi. Sementara itu, UU ITE mengatur kewajiban penyelenggara sistem elektronik, tetapi belum secara eksplisit menyebut penyedia platform konsultasi kesehatan online dan batasan tanggung jawab mereka dalam pengelolaan data medis. Akibatnya, terjadi tumpang tindih dan kekosongan pengaturan antarrezim hukum yang seharusnya saling melengkapi.

Dampak praktis dari celah ini adalah kesulitan dalam menentukan pihak yang paling bertanggung jawab ketika terjadi kebocoran atau penyalahgunaan data medis pasien. Kondisi ini menciptakan risiko *moral hazard*, di mana masing-masing pihak cenderung saling melepaskan tanggung jawab, sementara pasien tetap menanggung kerugian. Oleh karena itu, diperlukan pengaturan yang lebih tegas melalui peraturan pemerintah atau peraturan menteri yang secara rinci menguraikan pembagian tanggung jawab dalam layanan konsultasi kesehatan online. Pengaturan tersebut perlu mencakup tanggung jawab dokter dalam memilih platform yang aman dan memberikan *informed consent*, tanggung jawab fasilitas kesehatan dalam pengawasan dan audit, tanggung jawab penyedia platform dalam menjaga keamanan infrastruktur dan data, serta mekanisme koordinasi dan pertanggungjawaban bersama untuk menjamin perlindungan hukum yang efektif bagi pasien.

Celah 3: Pengaturan Rekam Medis Elektronik di Platform Pihak Ketiga

Meskipun UU Kesehatan mewajibkan penyelenggaraan rekam medis, pengaturannya masih berorientasi pada layanan kesehatan konvensional dan belum sepenuhnya mempertimbangkan karakteristik rekam medis elektronik dalam ekosistem digital. Undang-undang ini belum mengatur secara rinci aspek teknis penting seperti standar enkripsi data, mekanisme pencadangan (*backup*), pengendalian akses, masa retensi, serta tata cara penghapusan data medis elektronik yang dikelola oleh penyedia platform digital.

Selain aspek teknis, ketidakjelasan juga muncul terkait kepemilikan dan penguasaan rekam medis elektronik. Belum terdapat pengaturan yang tegas mengenai apakah pemilik rekam medis elektronik adalah dokter, fasilitas pelayanan kesehatan, pasien, atau penyedia platform. Ketidakjelasan ini berdampak pada penentuan pihak yang berwenang mengambil keputusan atas data medis, termasuk permintaan penghapusan, pembatasan akses, atau penggunaan data untuk kepentingan lain. Di samping itu, belum adanya pengaturan mengenai portabilitas data medis menyebabkan pasien tidak memiliki kepastian hukum untuk memindahkan data kesehatannya dari satu platform ke platform lain atau kepada dokter yang berbeda.

Dampak praktis dari celah pengaturan ini adalah terjadinya variasi kebijakan pengelolaan data antarplatform, yang berpotensi merugikan pasien dan mengganggu kesinambungan pelayanan kesehatan. Pasien dapat kehilangan akses terhadap riwayat medisnya secara utuh ketika berpindah dokter atau platform, sehingga berisiko menurunkan mutu pelayanan dan keselamatan pasien. Oleh karena itu, diperlukan pengaturan khusus melalui Peraturan Menteri Kesehatan yang secara komprehensif mengatur rekam medis elektronik dalam layanan konsultasi kesehatan online. Pengaturan tersebut perlu mencakup standar teknis penyimpanan, enkripsi, pencadangan, pengendalian akses, masa retensi, penghapusan data, kepemilikan, portabilitas, serta interoperabilitas sistem guna menjamin perlindungan hak pasien dan kontinuitas perawatan

kesehatan.

Celah 4: Koordinasi Pengawasan Antarinstansi

Isu Pokok: Tidak terdapat mekanisme koordinasi yang jelas dan formal antara instansi-instansi yang berwenang mengawasi perlindungan data medis pasien.

Manifestasi Celah:

- UU PDP diawasi oleh OJPP; UU Kesehatan diawasi oleh Kementerian Kesehatan; UU ITE diawasi oleh Kemenkominfo dan BRTI.
- Tidak ada MOU (Memorandum of Understanding) atau kerangka kerja formal yang mengatur bagaimana ketiga instansi ini berkoordinasi, melakukan investigasi bersama, dan berbagi informasi tentang pelanggaran di sektor konsultasi kesehatan online.

Dampak Praktis: Jika terjadi kebocoran data medis, berbagai pihak dapat memulai investigasi terpisah tanpa koordinasi yang baik, mengakibatkan duplikasi upaya dan inkonsistensi dalam kesimpulan. Hal ini juga membuka peluang bagi penyedia layanan untuk memanfaatkan celah koordinasi ini.

Diperlukan: Peraturan Presiden atau Keputusan Bersama Menteri Kesehatan, Menteri Komunikasi dan Informatika, dan OJPP yang mengatur: (a) mekanisme koordinasi pengawasan; (b) prosedur investigasi bersama; (c) prosedur berbagi informasi; dan (d) sinkronisasi dalam penegakan sanksi.

Celah 5: Perlindungan bagi Tenaga Kesehatan dalam Melaporkan Pelanggaran

Saat ini, pengawasan perlindungan data pribadi berada di bawah Otoritas Jaminan Perlindungan Data Pribadi, pengawasan pelayanan kesehatan berada pada Kementerian Kesehatan, sementara penyelenggaraan sistem elektronik diawasi oleh Kementerian Komunikasi dan Informatika beserta lembaga terkait. Namun, belum terdapat kerangka kerja formal, seperti nota kesepahaman atau regulasi khusus, yang mengatur koordinasi pengawasan, investigasi bersama, dan pertukaran informasi antarinstansi tersebut dalam konteks konsultasi kesehatan online. Akibatnya, pengawasan berjalan secara sektoral dan terpisah, tanpa integrasi yang memadai.

Dampak praktis dari lemahnya koordinasi ini terlihat ketika terjadi kebocoran atau penyalahgunaan data medis pasien. Berbagai instansi dapat melakukan investigasi secara terpisah tanpa sinkronisasi, yang berpotensi menimbulkan duplikasi upaya, perbedaan penilaian, dan inkonsistensi dalam penegakan sanksi. Kondisi ini juga membuka peluang bagi penyelenggara layanan konsultasi kesehatan online untuk memanfaatkan celah koordinasi antarinstansi guna menghindari tanggung jawab hukum. Oleh karena itu, diperlukan pengaturan pada tingkat kebijakan nasional, seperti Peraturan Presiden atau Keputusan Bersama Menteri Kesehatan, Menteri Komunikasi dan Informatika, dan Otoritas Jaminan Perlindungan Data Pribadi, yang secara tegas mengatur mekanisme koordinasi pengawasan, prosedur investigasi bersama, pertukaran informasi, serta sinkronisasi penegakan sanksi.

Selain persoalan koordinasi antarinstansi, terdapat pula celah hukum terkait perlindungan bagi tenaga kesehatan yang melaporkan pelanggaran perlindungan data medis pasien. Hingga saat ini, belum terdapat mekanisme perlindungan *whistleblower* yang secara khusus menjamin keamanan dan hak tenaga kesehatan yang melaporkan lemahnya sistem keamanan data di fasilitas atau platform konsultasi kesehatan online. Ketiadaan perlindungan ini menempatkan

tenaga kesehatan pada posisi rentan terhadap tindakan balasan, seperti intimidasi, mutasi, atau pemutusan hubungan kerja. Akibatnya, pelanggaran keamanan data berpotensi terus berlangsung tanpa terdeteksi. Oleh karena itu, diperlukan pengaturan yang memberikan perlindungan hukum bagi tenaga kesehatan pelapor, termasuk jaminan dari tindakan balasan, mekanisme pelaporan yang aman, serta insentif tertentu untuk mendorong keterbukaan demi perlindungan hak pasien.

KESIMPULAN

Kesimpulan

1. Berdasarkan uraian tersebut, dapat disimpulkan bahwa negara telah melakukan berbagai upaya hukum dan kebijakan untuk melindungi keamanan dan kerahasiaan data medis pasien dalam layanan konsultasi kesehatan online. Namun, upaya tersebut masih memerlukan penguatan melalui regulasi yang lebih spesifik, pengawasan yang ketat, serta peningkatan kapasitas sumber daya manusia. Sinergi antara negara, tenaga kesehatan, dan penyedia platform digital menjadi kunci utama keberhasilan perlindungan hukum data medis pasien. Dengan pendekatan yang komprehensif dan berkelanjutan, inovasi teknologi dalam pelayanan kesehatan dapat berkembang tanpa mengorbankan hak dasar dan martabat pasien.
2. Berdasarkan identifikasi berbagai permasalahan tersebut, dapat disimpulkan bahwa perlindungan hukum terhadap keamanan dan kerahasiaan data medis pasien dalam layanan konsultasi kesehatan online masih menghadapi tantangan struktural dan substansial. Kesenjangan regulasi, risiko keamanan siber, rendahnya literasi digital, serta lemahnya penegakan hukum menunjukkan perlunya pembenahan yang komprehensif. Penguatan regulasi yang adaptif, peningkatan kapasitas sumber daya manusia, serta pengawasan dan penegakan hukum yang efektif menjadi langkah strategis untuk menjamin perlindungan hak pasien. Dengan demikian, inovasi teknologi dalam pelayanan kesehatan dapat berjalan seiring dengan kepastian dan perlindungan hukum yang berkeadilan.
3. Pengaturan keamanan dan kerahasiaan data pasien pada konsultasi dokter online mengacu pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, serta Undang-Undang Informasi dan Transaksi Elektronik. UU Perlindungan Data Pribadi, Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, dan UU ITE secara normatif telah menempatkan kerahasiaan data rekam medis pasien sebagai bagian fundamental dari perlindungan hak asasi manusia dan fondasi hubungan kepercayaan antara pasien dan penyedia layanan kesehatan. Perlindungan data medis tidak hanya dipahami sebagai kewajiban hukum administratif, tetapi juga sebagai upaya menjaga martabat, privasi, serta hak pasien untuk mengendalikan informasi kesehatan pribadinya. Dalam konteks layanan konsultasi kesehatan online, kepercayaan pasien hanya dapat terbangun apabila terdapat jaminan bahwa data kesehatannya dikelola secara aman, bertanggung jawab, dan sesuai dengan prinsip perlindungan hukum. Meskipun UU ITE telah menyediakan kerangka hukum untuk menuntut ganti kerugian atas pelanggaran data, pengaturannya masih bersifat umum sehingga belum sepenuhnya mengakomodasi karakteristik data medis yang sangat sensitif. Oleh karena itu, harmonisasi dan penguatan pengaturan antara UU PDP, UU Kesehatan, dan UU ITE menjadi kebutuhan mendesak guna mewujudkan perlindungan hukum yang efektif, komprehensif, dan memberikan kepastian hukum bagi seluruh pihak dalam pelayanan kesehatan digital.

Saran

Berdasarkan penelitian ini perlu melakukan penguatan kerangka regulasi perlindungan data medis pasien dalam layanan konsultasi kesehatan online melalui pembentukan peraturan turunan yang lebih spesifik dan operasional. Pemerintah, khususnya Kementerian Kesehatan bekerja sama dengan kementerian dan lembaga terkait, perlu menetapkan standar teknis minimum keamanan data medis dalam telemedicine yang bersifat wajib, mencakup pengaturan enkripsi, pengendalian akses, pencatatan aktivitas sistem, manajemen risiko, serta mekanisme pemulihan data. Regulasi teknis ini diperlukan untuk menutup kesenjangan norma yang masih bersifat umum dalam undang-undang dan memberikan kepastian hukum bagi penyelenggara layanan serta perlindungan yang setara bagi pasien.

Selain penguatan regulasi, diperlukan peningkatan kapasitas dan koordinasi kelembagaan dalam pengawasan dan penegakan hukum. Negara perlu membangun mekanisme koordinasi yang jelas dan formal antara otoritas perlindungan data pribadi, Kementerian Kesehatan, dan instansi yang membidangi penyelenggaraan sistem elektronik agar pengawasan terhadap layanan kesehatan digital berjalan terpadu dan efektif. Penguatan pengawasan harus diikuti dengan penegakan sanksi yang konsisten dan proporsional terhadap pelanggaran keamanan dan kerahasiaan data medis, sehingga mampu menimbulkan efek jera dan meningkatkan kepatuhan hukum penyedia layanan.

Tenaga kesehatan dan penyedia platform layanan kesehatan digital juga perlu meningkatkan tanggung jawab profesional dan etika dalam pengelolaan data medis pasien. Tenaga kesehatan harus dibekali dengan peningkatan literasi digital dan pemahaman hukum terkait perlindungan data pribadi agar mampu menjalankan praktik konsultasi online secara aman dan bertanggung jawab. Di sisi lain, penyedia platform wajib menerapkan prinsip *privacy by design* dan *privacy by default* dalam seluruh tahapan pengembangan dan pengoperasian sistem, serta menyediakan mekanisme persetujuan (*informed consent*) yang transparan dan mudah dipahami oleh pasien. Dengan sinergi yang kuat antara negara, tenaga kesehatan, dan penyedia platform digital, perlindungan hukum terhadap keamanan dan kerahasiaan data medis pasien dapat terwujud secara efektif tanpa menghambat inovasi pelayanan kesehatan berbasis teknologi.

DAFTAR REFERENSI

1. Amalia, K. F., dkk. (2022). Scoping review: Hambatan penerapan telemedicine di Indonesia. *Bandung Conference Series: Medical Science*, 2(1).
2. Arif, M. A. I. (2018). *Tinjauan hukum atas layanan medis berbasis online* (Skripsi). Fakultas Hukum, Universitas Hasanuddin, Makassar.
3. Fariz, M. R. (2021). *Pola komunikasi dokter pada pasien melalui aplikasi Halodoc* (Skripsi). Fakultas Dakwah dan Komunikasi, UIN Ar-Raniri, Banda Aceh.
4. Ikatan Dokter Indonesia. (2012). *Kode etik kedokteran Indonesia*.
5. Jusuf, E. C., Kumala, R., & Adriano, A. (2023). Tinjauan hukum kerahasiaan rekam medis dalam laporan kesehatan ibu dan anak berbasis digital. *Wajah Hukum*, 7(1), 28.
6. Karo Karo, R., & Pasaribu, D. (2019). Aspek hukum konsultasi dokter melalui media online di Indonesia. *Tadaku Master Law Journal*, 3(2), 89–112.

7. Kichloo, A., Albosta, M., Dettloff, K., Wani, F., El-Amir, Z., Singh, J., Aljadah, M., Chakinala, R. C., Kanugula, A. K., Solanki, S., & Chugh, S. (2020). Telemedicine, the current COVID-19 pandemic and the future: A narrative review and perspectives moving forward in the USA. *Family Medicine and Community Health*, 8(3), 1–9. <https://doi.org/10.1136/fmch-2020-000530>
8. Kustiyanti, S. A. (2023). *Smart hospital: Konsep, implementasi, dan tantangan*. Dalam *Transformasi Rumah Sakit Indonesia Menuju Era Masyarakat 5.0* (hlm. 161).
9. Mangesti, Y. A. (2021). *Perlindungan hukum data pribadi pasien telemedicine*. Kompasiana. Diakses pada 1 Oktober 2025 dari <https://www.kompasiana.com>
10. Marzuki, P. M. (2008). *Penelitian hukum* (Edisi ke-4). Jakarta: Kencana.
11. Muhammad, S., Sosiawaty, I., Julia, P., & Patty, T. (2023). Analisis kinerja pelayanan kesehatan tenaga medis di Puskesmas Air Besar Negeri Batu Merah Kecamatan Sirimau Kota Ambon Provinsi Maluku. *Jurnal PROFESI*, 10(1), 197–210. <https://jurnal.unived.ac.id/index.php/prof/article/view/3740>
12. Pasaribu, K. F., Arisjulyanto, D., & H. B. T. (2017). Pengembangan telemedicine dalam mengatasi konektivitas dan aksesibilitas pelayanan kesehatan. *Berita Kedokteran Masyarakat (BKM Public Health and Community Medicine)*, 2010(2015), 42–58.
13. Ramdoni, M. M., & Herdiansyah, M. I. (2023). Pengembangan sistem informasi konsultasi dokter menggunakan framework Laravel. *Journal of Information System Research (JOSH)*, 4(3), 831–839. <https://doi.org/10.47065/josh.v4i3.3276>
14. Uscher-Pines, L., Mulcahy, A., Cowling, D., Hunter, G., Burns, R., & Mehrotra, A. (2016). Access and quality of care in direct-to-consumer telemedicine. *Telemedicine and E-Health*, 22(4), 282–287. <https://doi.org/10.1089/tmj.2015.0079>
15. Widiarty, S., & Wiwik, I. A. (2024). *Buku ajar: Metode penelitian hukum*. Publika.

Peraturan Perundang-undangan

1. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
2. Peraturan Menteri Kesehatan Nomor 20 Tahun 2019 tentang Penyelenggaraan Konsultasi kesehatan online antara Fasilitas Pelayanan Kesehatan.
3. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik.