

Analisis Yuridis Kebocoran Data di Layanan Kesehatan Digital: Studi Kasus Aplikasi Telemedicine di Indonesia

Aenun Nadiroh¹, Sidi Ahyar Wiraguna²

¹Fakultas Ilmu Komunikasi Universitas Esa Unggul Jakarta

²Fakultas Hukum Universitas Esa Unggul Jakarta

Jl. Arjuna Utara Nomor 9, Kebon Jeruk, Jakarta Barat-11510

Email: aennunadiroh2006@gmail.com¹, adipatiwiraguna@gmail.com²

Abstract: *The development of telemedicine services in Indonesia has become an innovative solution in providing remote healthcare access, particularly since the COVID-19 pandemic. However, behind this progress lies a serious legal issue regarding the leakage of patients' personal data, which remains inadequately addressed. This study aims to analyze the legal aspects of personal data protection in telemedicine services using a normative legal approach, focusing on statutory regulations such as Law No. 27 of 2022 on Personal Data Protection and related health sector policies. The findings indicate that, despite the presence of a formal legal framework, practical implementation remains weak, as evidenced by multiple data breach incidents, including the e-HAC and COVID-19 patient medical record cases. Existing technical regulations fall short in addressing the complexity of digital systems, while awareness among service providers regarding privacy and accountability principles remains insufficient. Therefore, the protection of patient data must be seen as an integral part of digital medical services through effective legal enforcement and the strengthening of ethical and transparent data governance.*

Abstract: Perkembangan layanan telemedicine di Indonesia telah menjadi solusi inovatif dalam menghadirkan akses kesehatan jarak jauh, khususnya sejak pandemi COVID-19. Namun, di balik kemajuan ini, muncul isu hukum serius terkait kebocoran data pribadi pasien yang belum sepenuhnya teratasi. Penelitian ini bertujuan untuk menganalisis aspek yuridis dari perlindungan data pribadi pasien dalam layanan telemedicine, dengan pendekatan hukum normatif yang berfokus pada studi peraturan perundang-undangan seperti UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan regulasi terkait sektor kesehatan. Hasil kajian menunjukkan bahwa meskipun terdapat kerangka hukum formal, implementasi di lapangan masih lemah, terbukti dari berbagai insiden kebocoran data, termasuk kasus e-HAC dan data rekam medis pasien COVID-19. Regulasi teknis belum sepenuhnya mengantisipasi kompleksitas sistem digital, sementara kesadaran penyedia layanan terhadap prinsip privasi dan akuntabilitas masih rendah. Oleh karena itu, perlindungan data pasien harus menjadi bagian integral dari pelayanan medis digital melalui penegakan hukum yang efektif dan penguatan tata kelola data yang etis dan transparan.

Article History

Received: April 30, 2025

Revised: May 10, 2025

Published: May 17, 2025

Keywords: *Telemedicine, Personal Data Protection, Health Law, PDP Law, Patient Data Breach.*

Kata kunci: Telemedicine, Perlindungan Data Pribadi, Hukum Kesehatan, UU PDP, Kebocoran Data Pasien.



<https://doi.org/10.5281/zenodo.15520536>

This is an open-access article under the [CC-BY-SA License](#).

PENDAHULUAN

Perkembangan teknologi digital telah membawa perubahan signifikan dalam dunia pelayanan kesehatan, salah satunya adalah kemunculan dan pertumbuhan layanan telemedicine di Indonesia. Telemedicine merupakan solusi layanan kesehatan jarak jauh berbasis teknologi yang memungkinkan pasien dan tenaga medis saling terhubung tanpa perlu tatap muka langsung. Layanan ini menjadi semakin relevan dan mendesak untuk diterapkan, terutama saat Indonesia menghadapi pandemi COVID-19 yang membatasi mobilitas masyarakat serta menuntut adaptasi terhadap sistem layanan kesehatan konvensional. Data menunjukkan bahwa pada tahun 2019 jumlah pengguna layanan telemedicine di Indonesia hanya sekitar dua juta orang.³ Namun, selama masa pandemi, jumlah ini

¹ 8111422718, Fakultas Hukum Universitas Negeri Semarang

² 8111422728, Fakultas Hukum Universitas Negeri Semarang

³ Ulfathea Mulyadita et al., "Mapping Telemedicine in Indonesia: Evidence for Policy Action at a Critical Juncture," 2025.

melonjak drastis hingga mencapai 20 juta pengguna pada tahun 2020. Bahkan pascapandemi, tren penggunaannya tidak mengalami penurunan, melainkan terus meningkat, dengan laporan peningkatan hingga 78,8% di berbagai fasilitas pelayanan kesehatan.⁴

Layanan telemedicine kini telah terintegrasi ke dalam sistem pelayanan kesehatan nasional. Pada tahun 2024, tercatat sebanyak 63 rumah sakit dan 174 puskesmas telah mengimplementasikan layanan telemedicine secara resmi, dan sekitar 74% rumah sakit di Indonesia menyediakan layanan konsultasi kesehatan jarak jauh.⁵ Platform telemedicine pun semakin beragam, baik yang dikembangkan oleh pemerintah seperti Sisrute, KOMEN, TEMENIN, dan Sehatpedia, maupun swasta seperti Halodoc, Alodokter, dan SehatQ yang populer di kalangan masyarakat. Tidak hanya layanan konsultasi umum, kini tersedia juga teknologi pendukung lain seperti tele-radiology, tele-ECG, tele-ICU, mobile clinics, hingga IoT ambulance. Inovasi-inovasi tersebut menunjukkan potensi besar telemedicine dalam meningkatkan akses dan kualitas pelayanan kesehatan, terutama di wilayah terpencil yang sulit dijangkau secara langsung oleh tenaga medis.

Selain kemudahan akses, efisiensi waktu dan biaya, serta kemampuan untuk melakukan pemantauan kesehatan jangka panjang bagi pasien penyakit kronis, telemedicine juga menjadi alat penting dalam mengurangi penyebaran penyakit menular. Namun, di tengah manfaat yang sangat besar ini, terdapat pula tantangan serius yang harus dihadapi, salah satunya adalah perlindungan data pribadi pasien. Meskipun penetrasi internet di Indonesia telah mencapai 79,5% dan mayoritas masyarakat memiliki akses ke smartphone, masih terdapat ketimpangan distribusi infrastruktur antara wilayah urban dan rural.⁶ Konektivitas yang terbatas serta minimnya perangkat digital di beberapa daerah menjadi kendala tersendiri dalam pemerataan layanan. Lebih dari itu, sistem keamanan digital dalam platform telemedicine masih banyak menyimpan celah yang rentan terhadap pelanggaran dan kebocoran data pribadi.

Sejumlah insiden kebocoran data yang terjadi dalam beberapa tahun terakhir semakin mempertegas kelemahan sistem keamanan data layanan kesehatan digital di Indonesia. Salah satu kasus paling mencolok terjadi pada awal tahun 2022, ketika data rekam medis milik sekitar enam juta pasien COVID-19 bocor dan tersebar di dunia maya. Data tersebut memiliki ukuran hingga 720 GB dan berisi informasi sangat sensitif, seperti nama lengkap, hasil tes laboratorium, foto medis, riwayat penyakit, hingga surat persetujuan isolasi dari BPJS.⁷ Dampak dari kebocoran data ini sangat serius, karena informasi medis yang bersifat pribadi bisa dimanfaatkan untuk pencurian identitas, penipuan finansial, hingga menyebabkan tekanan psikologis bagi korban. Belum tuntas penanganan kasus tersebut, publik kembali dikejutkan oleh kasus kebocoran data dari aplikasi e-HAC pada tahun 2021 yang turut mengekspos data pribadi lebih dari satu juta orang, mencakup hasil tes PCR, nomor identitas, dan informasi sensitif lainnya.⁸

Tak hanya kasus besar, risiko kebocoran data juga muncul dari praktik harian konsultasi telemedicine. Penelitian dari Kaspersky menunjukkan bahwa sekitar 30% penyedia layanan kesehatan di Indonesia mengalami kasus di mana pegawainya secara tidak sengaja atau lalai membahayakan data pasien selama proses telemedicine berlangsung.⁹ Banyak dokter yang menggunakan platform komunikasi umum seperti WhatsApp, Zoom, atau FaceTime yang sejatinya tidak didesain untuk layanan kesehatan dan tidak memiliki protokol keamanan informasi yang memadai. Hal ini membuka

⁴ Widya Hapsari Murima et al., "Penggunaan Telemedicine Di Fasilitas Kesehatan Selama Pandemi Covid-19," *Indonesian Journal of Health Administration* 10, no. 2 (2022).

⁵ Rita Pusputa Sari, "Telehealth Dan Telemedicine: Solusi Akses Kesehatan Digital," *Cloudcomputing.Id*, 2025, <https://www.cloudcomputing.id/berita/telehealth-solusi-kesehatan-digital>.

⁶ Mulyadita et al., "Mapping Telemedicine in Indonesia: Evidence for Policy Action at a Critical Juncture."

⁷ Smsul Arifin, "Melindungi Privasi Di Era Digital: Mengatasi Kebocoran Data Rekam Medis Pasien COVID-19," *Jatim.Tribunnews.Com*, 2025, <https://jatim.tribunnews.com/2025/01/08/melindungi-privasi-di-era-digital-mengatasi-kebocoran-data-rekam-medis-pasien-covid-19>.

⁸ Kliwantoro and Chandra Hamdani Noor, "Pakar Nilai Respons Kemenkes Lambat Terkait Laporan Kebocoran Data," *Antaranews.Com*, 2021, <https://www.antarnews.com/berita/2365010/pakar-nilai-respons-kemenkes-lambat-terkait-laporan-kebocoran-data>.

⁹ CNN, "Waspada, Data Pribadi Pasien Potensi Bocor Saat Konsultasi Telehealth," *Cnnindonesia.Com*, 2022, <https://www.cnnindonesia.com/teknologi/20220105182546-185-743027/waspada-data-pribadi-pasien-potensi-bocor-saat-konsultasi-telehealth>.

celah besar bagi kebocoran data, baik oleh serangan siber dari pihak ketiga maupun akibat kesalahan penggunaan dari internal institusi kesehatan itu sendiri.

Pemerintah Indonesia melalui Kementerian Kominfo, Kementerian Kesehatan, serta Badan Siber dan Sandi Negara (BSSN) telah berupaya untuk menanggapi isu ini dengan investigasi, pembentukan regulasi, dan kerja sama lintas lembaga. Beberapa regulasi seperti Permenkes No. 20 Tahun 2019 dan Keputusan Menteri Kesehatan tentang penyelenggaraan layanan telemedicine telah diterbitkan sebagai dasar hukum pelaksanaan. Selain itu, pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjadi tonggak penting dalam perlindungan hak-hak individu atas informasi pribadinya, termasuk dalam konteks layanan kesehatan.

Penelitian yang dilakukan oleh Wiraguna, Sulaiman, dan Barthos mengenai implementasi UU No. 27 Tahun 2022 dalam sektor e-commerce memberikan gambaran bahwa sektor digital di Indonesia mulai melakukan penyesuaian kebijakan dan infrastruktur teknologinya untuk menjamin keamanan data pribadi konsumen. Meskipun fokus kajian tersebut berada pada ranah perdagangan elektronik, temuan mereka memberikan relevansi yang signifikan bagi sektor layanan kesehatan digital—seperti telemedicine—karena kedua sektor sama-sama mengelola data pribadi dalam jumlah besar dan bersifat sensitif. Sebagaimana e-commerce dituntut untuk meningkatkan sistem perlindungan data melalui kebijakan privasi dan teknologi keamanan, demikian pula penyedia layanan kesehatan digital harus memperkuat sistem perlindungan data pasien.¹⁰ Hal ini menunjukkan bahwa implementasi UU PDP tidak hanya memberikan kerangka hukum umum, tetapi juga menuntut kesiapan sektoral dalam menerapkan prinsip-prinsip perlindungan data, termasuk peningkatan kesadaran pengguna dan tenaga profesional terhadap hak serta kewajiban yang diatur dalam undang-undang. Dengan demikian, pembelajaran dari sektor e-commerce dapat menjadi acuan awal dalam mengevaluasi kesiapan dan tantangan implementasi perlindungan data pribadi di sektor kesehatan.

Namun, pada kenyataannya, penguatan regulasi dan sistem pengawasan yang terstruktur masih dibutuhkan, karena kasus kebocoran data tetap saja terjadi dan penyelesaiannya cenderung lambat dan tidak transparan. Hal ini menimbulkan kekhawatiran di kalangan masyarakat dan menurunkan kepercayaan terhadap layanan kesehatan digital, padahal kepercayaan adalah fondasi utama dalam hubungan antara pasien dan penyedia layanan.¹¹

Dengan mempertimbangkan kompleksitas permasalahan di atas, maka tulisan ini bertujuan untuk menganalisis aspek yuridis dari kebocoran data pribadi pasien yang terjadi dalam layanan telemedicine di Indonesia. Penelitian ini secara khusus akan mengkaji ketentuan hukum yang berlaku, studi kasus kebocoran data di aplikasi telemedicine, serta tanggung jawab hukum dari penyedia layanan atas insiden tersebut. Harapannya, artikel ini dapat memberikan kontribusi dalam penguatan regulasi perlindungan data di sektor kesehatan digital, serta menjadi masukan bagi para pemangku kebijakan dalam menciptakan sistem yang aman dan terpercaya bagi seluruh pengguna layanan kesehatan berbasis teknologi.

METODE PENELITIAN

Penelitian ini menggunakan metode pendekatan hukum normatif, yaitu pendekatan yang menitikberatkan pada studi terhadap norma-norma hukum yang tertulis dalam peraturan perundang-undangan, asas hukum, maupun doktrin-doktrin yang berkembang dalam ilmu hukum.¹² Pendekatan ini bertujuan untuk mengkaji bagaimana pengaturan telemedicine dan perlindungan data pasien diatur dalam sistem hukum Indonesia, khususnya melalui analisis terhadap Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit, serta regulasi pelaksana seperti Peraturan Menteri Kesehatan. Pendekatan normatif digunakan karena dapat memberikan landasan yuridis yang sistematis, membantu peneliti dalam

¹⁰ Sidi Ahyar Wiraguna, Abdullah Sulaiman, and Megawati Barthos, "Implementation of Consumer Personal Data Protection in Ecommerce from the Perspective of Law No. 27 of 2022," *Journal of World Science* 3, no. 3 (2024): 410–18, doi:10.58344/jws.v3i3.584.

¹¹ Arief Budiman, Muzakar Isa, and Siti Soekiswati, "Analisis Risiko Dan Tindakan Pencegahan Kebocoran Data Rekam Medis Elektronik Pasien Di RS P Surakarta," *Ranah Research: Journal of Multidisciplinary Research and Development* 7, no. 3 (2025): 2118–27.

¹² Sidi Ahyar Wiraguna, "Metode Normatif Dan Empiris Dalam Penelitian Hukum: Studi Eksploratif Di Indonesia" 3, no. 3 (2024), doi:10.59818/jps.v3i3.1390.

mengidentifikasi celah hukum, serta mengevaluasi kecukupan norma terhadap perkembangan teknologi layanan kesehatan jarak jauh.

Pendekatan normatif unggul dalam memberikan kerangka hukum yang jelas dan terstruktur, namun memiliki keterbatasan dalam menangkap dinamika sosial dan empiris di masyarakat. Hal ini menjadi penting ketika membahas isu kebocoran data dan keamanan privasi dalam telemedicine, yang bukan hanya berdimensi legal formal, melainkan juga menyentuh aspek sosial, teknologi, dan kepercayaan publik.¹³ Meskipun begitu, pendekatan normatif tetap relevan dalam konteks penelitian ini karena fokus utama penelitian adalah menelaah substansi hukum yang berlaku dan mengevaluasi sejauh mana regulasi tersebut mampu memberikan perlindungan hukum terhadap pasien sebagai subjek hukum dalam praktik layanan telemedicine.

PEMBAHASAN

A. Tinjauan Hukum terhadap Perlindungan Data Pribadi Pasien dalam Layanan Telemedicine di Indonesia

Dalam era digitalisasi pelayanan kesehatan, perlindungan data pribadi pasien menjadi aspek krusial yang harus mendapatkan perhatian serius, khususnya dalam penyelenggaraan layanan telemedicine. Data pribadi, sebagaimana diatur dalam Pasal 1 angka 1 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), adalah setiap data tentang seseorang yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya. Dalam konteks layanan kesehatan digital, data pribadi mencakup nama pasien, alamat, nomor rekam medis, dan informasi kontak. Adapun data pribadi sensitif atau data pribadi spesifik—sebagaimana dijelaskan dalam Pasal 4 ayat (2) UU PDP—meliputi data kesehatan, data biometrik, dan data genetika, yang apabila disalahgunakan dapat menimbulkan risiko serius terhadap individu. Oleh karena itu, perlindungan terhadap data ini wajib dilaksanakan dengan standar keamanan tinggi dan kepatuhan hukum yang ketat.¹⁴

Kerangka hukum Indonesia telah menyediakan beberapa landasan regulatif yang mengatur perlindungan data pasien, terutama dalam ranah telemedicine. UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang telah diperbarui melalui UU Nomor 19 Tahun 2016, menegaskan pentingnya keamanan sistem elektronik dan perlindungan data dalam transaksi digital. Lebih spesifik lagi, UU Nomor 36 Tahun 2009 tentang Kesehatan menyebutkan dalam Pasal 57 bahwa setiap orang berhak atas kerahasiaan kondisi kesehatan pribadinya, dan penyedia layanan berkewajiban menjaga informasi medis pasien. Regulasi teknis lebih lanjut dijabarkan dalam Peraturan Menteri Kesehatan Republik Indonesia, seperti Permenkes No. 20 Tahun 2019 tentang Penyelenggaraan Pelayanan Telemedicine Antar Fasilitas Pelayanan Kesehatan, serta Permenkes No. 24 Tahun 2022 tentang Rekam Medis, yang mengatur tata kelola informasi kesehatan secara digital. UU PDP sendiri memperkenalkan prinsip-prinsip fundamental perlindungan data, termasuk keterbukaan, tujuan terbatas, minimisasi data, keamanan data, persetujuan eksplisit, serta hak akses dan koreksi oleh subjek data (Pasal 20–29). Dalam kerangka ini, penyedia layanan telemedicine bertindak sebagai pengendali data (data controller) yang wajib menjamin keamanan, keakuratan, serta penggunaan data secara sah dan transparan.

Kewajiban hukum yang diemban oleh penyedia layanan mencakup pengamanan data melalui teknologi seperti enkripsi, firewall, dan kontrol akses berbasis otorisasi, sebagaimana ditekankan dalam Pasal 39 UU PDP. Selain itu, setiap pengumpulan dan pemrosesan data harus memperoleh persetujuan eksplisit dari pasien sebagaimana diatur dalam Pasal 20 UU PDP. Penyelenggara telemedicine juga diwajibkan melakukan Penilaian Dampak Privasi (*Privacy Impact Assessment*) guna mengidentifikasi potensi risiko kebocoran data sejak awal. Tidak kalah penting, apabila terjadi pelanggaran atau insiden kebocoran data, pengendali data wajib melaporkan kepada otoritas berwenang dan memberi notifikasi

¹³ Ibid.

¹⁴ Edy Susanto, Adhani Windari, and Rizkiyatul Amalia, “EDIKASI: Empowering Data Integrity and Knowledge on Health Information Release in the Digital Era,” *LINK* 20, no. 2 (2024): 113–17.

kepada pemilik data, seperti tertuang dalam Pasal 46 UU PDP.¹⁵ Ketentuan ini bertujuan menjamin transparansi dan akuntabilitas dalam perlindungan data pasien. Kewajiban lainnya meliputi pelatihan sumber daya manusia, pemeliharaan rekam medis yang hanya dapat diakses oleh pihak berwenang, serta audit rutin terhadap sistem keamanan.

Meski secara normatif Indonesia telah memiliki kerangka hukum yang cukup memadai, pelaksanaan di lapangan masih menghadapi sejumlah kendala. Seperti yang diungkapkan oleh Wiraguna, pendekatan normatif memang unggul dalam memberikan struktur hukum yang jelas dan terstandarisasi, tetapi tidak sepenuhnya mampu menangkap dinamika sosial dan praktik nyata di lapangan yang terus berubah dengan cepat.¹⁶ Sebaliknya, pendekatan empiris justru lebih adaptif terhadap realitas tersebut, meski di sisi lain kerap menghadapi kendala validitas dan ketidakseragaman data. Dalam hal perlindungan data kesehatan digital, kelemahan terbesar regulasi adalah belum adanya aturan khusus yang secara rinci mengatur teknis perlindungan data dalam telemedicine, serta masih rendahnya kesiapan infrastruktur teknologi dan kapasitas sumber daya manusia di banyak fasilitas kesehatan. Selain itu, tantangan keamanan siber yang terus meningkat belum sepenuhnya terakomodasi oleh perangkat hukum yang ada, menimbulkan celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, diperlukan penguatan regulasi sektoral, peningkatan literasi digital baik bagi penyedia maupun pengguna layanan, serta penerapan standar keamanan digital yang konsisten agar perlindungan data pasien benar-benar terjamin dalam praktik.

B. Analisis Kasus Kebocoran Data Pasien di Aplikasi Telemedicine

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

Kebocoran data semacam ini sangat berisiko karena menyangkut hak privasi pasien atas informasi medisnya. Berdasarkan Pasal 58 ayat (1) dan (2) Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, setiap orang berhak atas kerahasiaan data dan informasi pribadi yang diberikan kepada tenaga kesehatan dan fasilitas pelayanan kesehatan. Bahkan dalam konteks perlindungan data pribadi secara umum, Pasal 2 dan Pasal 4 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dengan tegas menyebutkan bahwa setiap pengendali data wajib menjamin keamanan data pribadi yang berada dalam penguasaannya, serta melindungi data dari akses, pengungkapan, dan penggunaan tanpa izin. Artinya, insiden ini jelas melanggar hak-hak fundamental pasien dan menyalahi kewajiban pengelola data.¹⁸

Penyebab kebocoran data dalam kasus ini dapat dianalisis dari beberapa aspek. Dari sisi teknis, kelemahan dalam sistem keamanan teknologi informasi menjadi akar masalah utama. Banyak rumah sakit dan penyedia layanan kesehatan digital belum menggunakan sistem enkripsi yang kuat dan tidak melakukan audit keamanan secara berkala. Server yang digunakan juga sering kali tidak memiliki proteksi berlapis yang memadai terhadap potensi serangan siber. Selain itu, dari sisi sumber daya manusia, masih banyak tenaga medis dan administratif yang kurang memahami pentingnya menjaga

¹⁵ Calvin Anthony Putra and Muhammad Ali Masnun, "Analisis Pertanggungjawaban Rumah Sakit Terkait Potensi Kebocoran Data Rekam Medis Elektronik Akibat Cyber Crime," *Novum: Jurnal Hukum* 9, no. 2 (2022): 191–200.

¹⁶ Wiraguna, "Metode Normatif Dan Empiris Dalam Penelitian Hukum : Studi Eksploratif Di Indonesia."

¹⁷ Lensa Nurjanah, "Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik Di Rumah Sakit Bethesda Yoyakarta," 2023.

¹⁸ Novita Indriyani, "Analisis Aspek Keamanan Data Pada SIMARS Dalam Penerapan Rekam Medis Elektronik Di RSUP Prof. Dr. IGNG Ngurah Denpasar," 2023.

kerahasiaan data pasien. Pelatihan yang minim dan prosedur yang belum baku membuat kelalaian menjadi celah potensial bagi kebocoran. Dari aspek kelembagaan, kurangnya regulasi teknis yang spesifik dan lemahnya koordinasi antarlembaga juga memperbesar kemungkinan terjadinya kebocoran. Tidak kalah penting, ancaman eksternal seperti serangan hacker memanfaatkan kelemahan sistem ini untuk mencuri dan memperjualbelikan data, sebagaimana pernah terungkap dalam kasus kebocoran data BPJS Kesehatan yang lebih dulu terjadi.

Pemerintah merespons kasus ini dengan melibatkan Kementerian Komunikasi dan Informatika (Kominfo), Kementerian Kesehatan (Kemenkes), serta Badan Siber dan Sandi Negara (BSSN) untuk melakukan investigasi dan penguatan sistem keamanan. Kominfo mendorong percepatan implementasi UU PDP dengan menetapkan ketentuan pidana maupun administratif terhadap pelanggaran, seperti disebut dalam Pasal 67 sampai Pasal 73 UU PDP yang mengatur sanksi pidana dan denda hingga miliaran rupiah bagi pihak yang lalai atau menyalahgunakan data pribadi. Sementara itu, Kemenkes merilis pedoman teknis pengelolaan rekam medis elektronik dan standar perlindungan data kesehatan, sebagai bagian dari upaya memperkuat ekosistem telemedicine yang aman dan terpercaya.

Namun, efektivitas dari respons ini masih dipertanyakan. Di lapangan, penerapan standar keamanan data belum merata dan masih terdapat banyak penyedia layanan yang belum memenuhi persyaratan minimum perlindungan data. Meskipun adanya regulasi merupakan langkah maju, pengawasan dan penegakan hukum yang lemah membuat regulasi tersebut belum berdampak signifikan. Hal ini berdampak langsung terhadap kepercayaan publik. Banyak masyarakat merasa ragu dan khawatir menggunakan layanan telemedicine karena takut data kesehatannya disalahgunakan. Dalam jangka panjang, hal ini dapat menghambat digitalisasi layanan kesehatan dan merugikan upaya pemerintah dalam meningkatkan akses pelayanan kesehatan berbasis teknologi.

Dengan mempertimbangkan semua hal tersebut, dapat disimpulkan bahwa kasus kebocoran data pasien dalam aplikasi telemedicine mencerminkan kelemahan sistemik dalam tata kelola data kesehatan digital di Indonesia. Tidak hanya melanggar hak konstitusional warga atas perlindungan privasi, tetapi juga menciptakan ketidakpercayaan yang dapat merusak ekosistem layanan kesehatan berbasis teknologi. Oleh karena itu, diperlukan upaya komprehensif mulai dari penguatan regulasi yang lebih rinci untuk sektor kesehatan digital, peningkatan sistem keamanan teknologi, pelatihan intensif bagi tenaga kesehatan, serta edukasi kepada masyarakat mengenai hak-hak mereka atas data pribadi. Ke depan, perlindungan data pasien tidak boleh dianggap sebagai isu teknis semata, tetapi harus menjadi prioritas utama dalam menjamin pelayanan kesehatan yang bermartabat dan berkeadilan.

C. Tanggung Jawab Hukum Penyedia Layanan Telemedicine dan Implikasinya terhadap Regulasi

Dalam sistem pelayanan kesehatan digital yang semakin berkembang pesat, tanggung jawab hukum penyedia layanan telemedicine menjadi sorotan penting, terutama menyangkut perlindungan data pasien, kualitas pelayanan medis, dan kepatuhan terhadap regulasi. Penyedia layanan telemedicine, baik yang berbentuk aplikasi digital, rumah sakit, maupun tenaga kesehatan individu, memiliki tanggung jawab hukum yang melekat sebagaimana diatur dalam berbagai peraturan perundang-undangan yang berlaku di Indonesia. Secara prinsip, mereka wajib menjamin keamanan data pribadi pasien, memberikan layanan kesehatan sesuai standar profesi, serta mematuhi ketentuan administratif dan teknis yang telah ditetapkan oleh pemerintah. Ketentuan ini dapat ditemukan dalam Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, khususnya Pasal 161 ayat (1), yang menyatakan bahwa pelayanan kesehatan berbasis teknologi informasi dan komunikasi wajib memenuhi standar mutu pelayanan kesehatan, perlindungan data pribadi, serta keselamatan pasien.¹⁹ Hal ini menunjukkan bahwa penyedia layanan telemedicine tidak hanya bertanggung jawab secara moral, tetapi juga secara hukum atas segala bentuk risiko dan konsekuensi hukum dari layanan yang mereka berikan.

Lebih lanjut, tanggung jawab hukum penyedia layanan telemedicine juga ditegaskan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Dalam Pasal

¹⁹ Alaikha Annan, "Tinjauan Yuridis Perlindungan Data Pribadi Pada Sektor Kesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022," *Synergy: Jurnal Ilmiah Multidisiplin* 1, no. 04 (2024): 247–54.

39, disebutkan bahwa pengendali data pribadi wajib menjaga kerahasiaan data yang berada dalam penguasaannya dan dilarang memproses data pribadi untuk tujuan lain tanpa persetujuan subjek data. Dalam konteks telemedicine, ini berarti setiap informasi yang dikumpulkan, disimpan, atau diproses melalui aplikasi atau platform digital harus mendapatkan persetujuan eksplisit dari pasien, serta harus digunakan hanya untuk tujuan pelayanan kesehatan yang dimaksud.²⁰ Jika penyedia layanan terbukti lalai atau menyalahgunakan data pasien, maka sanksi pidana dan administratif dapat diberlakukan sebagaimana tercantum dalam Pasal 67 sampai Pasal 73 UU PDP. Sanksi tersebut mencakup denda hingga miliaran rupiah dan hukuman penjara bagi pelaku pelanggaran yang bersifat serius.

Selain aspek perlindungan data, tanggung jawab hukum juga mencakup kewajiban memberikan pelayanan yang sesuai dengan standar profesi kedokteran dan etika kesehatan. Pasal 70 Undang-Undang Kesehatan Tahun 2023 mewajibkan tenaga kesehatan, termasuk yang bekerja melalui platform digital, untuk menjunjung tinggi keselamatan pasien serta bertanggung jawab atas segala tindakan medis yang dilakukan. Dalam hal terjadi malpraktik atau kelalaian yang menyebabkan kerugian pada pasien, penyedia layanan tetap dapat dimintai pertanggungjawaban hukum, baik secara perdata maupun pidana. Dalam praktiknya, bentuk tanggung jawab ini sering kali mencakup kewajiban ganti rugi, pencabutan izin praktik, hingga tuntutan hukum apabila terbukti terjadi pelanggaran terhadap hak pasien.

Implikasi dari tanggung jawab hukum ini terhadap regulasi sangat signifikan. Negara dituntut untuk menyediakan kerangka hukum yang tegas dan spesifik terkait telemedicine agar tidak menimbulkan kekosongan hukum atau tumpang tindih antara peraturan. Pemerintah telah merespons hal ini dengan mengeluarkan Peraturan Menteri Kesehatan (Permenkes) Nomor 24 Tahun 2022 tentang Rekam Medis, yang di dalamnya mengatur tata cara penyimpanan dan pengelolaan rekam medis elektronik secara aman dan rahasia. Namun, masih dibutuhkan regulasi yang lebih komprehensif dan adaptif terhadap dinamika digitalisasi kesehatan, seperti pedoman teknis pengamanan sistem elektronik, prosedur tanggap insiden kebocoran data, dan kewajiban pelaporan berkala bagi penyedia layanan. Tanpa regulasi yang memadai dan pengawasan yang ketat, maka tanggung jawab hukum hanya akan menjadi konsep normatif yang sulit diimplementasikan di lapangan.

Oleh karena itu, penting bagi semua pemangku kepentingan, termasuk penyedia layanan telemedicine, regulator, dan masyarakat, untuk membangun ekosistem hukum yang tidak hanya melindungi hak-hak pasien, tetapi juga memberikan kepastian hukum bagi pelaku usaha dan tenaga kesehatan. Tanggung jawab hukum penyedia layanan telemedicine bukan sekadar kewajiban administratif, melainkan pilar utama dalam menjamin kepercayaan publik terhadap pelayanan kesehatan digital. Hanya dengan kepatuhan yang tinggi terhadap regulasi dan kesadaran hukum yang kuat, telemedicine dapat berkembang sebagai solusi kesehatan yang inovatif, aman, dan bermutu di Indonesia.

SIMPULAN

Berdasarkan uraian yang telah disampaikan, dapat disimpulkan bahwa perlindungan data pribadi pasien dalam layanan telemedicine di Indonesia merupakan isu yang sangat penting dan penuh tantangan, seiring dengan semakin masifnya digitalisasi sektor kesehatan. Meskipun secara normatif Indonesia telah memiliki kerangka regulasi seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang Kesehatan, serta beberapa peraturan teknis dari Kementerian Kesehatan, keberadaan aturan-aturan tersebut belum sepenuhnya menjawab kebutuhan riil di lapangan.

Sebagaimana dibahas dalam Tinjauan Hukum, perlindungan data dalam telemedicine telah mendapatkan perhatian dari sisi regulatif, terutama dengan diaturnya kewajiban pengendali data untuk menjaga keamanan, memperoleh persetujuan eksplisit, dan melaporkan insiden kebocoran. Namun, implementasi prinsip-prinsip hukum ini masih terkendala oleh minimnya infrastruktur keamanan

²⁰ Ibid.

digital, kurangnya standardisasi teknis perlindungan data di sektor kesehatan, serta rendahnya kapasitas dan kesadaran hukum dari penyedia layanan itu sendiri.

Di sisi lain, melalui pembahasan kasus nyata, seperti kebocoran data pada sistem e-HAC dan rekam medis pasien COVID-19, tampak jelas bahwa tata kelola data pribadi dalam layanan telemedicine masih menyimpan celah sistemik. Insiden-insiden tersebut tidak hanya mencerminkan kegagalan teknis, tetapi juga lemahnya pengawasan dan koordinasi antarlembaga, serta lambatnya penanganan dan pemulihan dari pihak pemerintah dan penyedia layanan. Akibatnya, kepercayaan publik terhadap layanan kesehatan digital mengalami erosi, padahal kepercayaan merupakan pondasi utama dalam relasi antara pasien dan penyedia layanan medis.

Oleh karena itu, perlindungan data pribadi pasien tidak dapat hanya diposisikan sebagai kepatuhan administratif terhadap regulasi, tetapi harus dipandang sebagai pilar utama dalam menjamin mutu, etika, dan legitimasi pelayanan telemedicine. Ke depan, diperlukan pembaruan regulasi yang lebih komprehensif dan responsif terhadap karakteristik sektor kesehatan digital, disertai dengan penguatan infrastruktur siber, peningkatan literasi digital dan hukum, serta sistem pengawasan dan penegakan hukum yang tegas. Hanya dengan komitmen kolektif dari seluruh pemangku kepentingan—negara, penyedia layanan, dan masyarakat—maka perlindungan hak atas privasi pasien dapat benar-benar diwujudkan dalam ekosistem layanan kesehatan digital yang adil, aman, dan terpercaya.

DAFTAR PUSTAKA

- Ahyar Wiraguna, Sidi, Abdullah Sulaiman, and Megawati Barthos. "Implementation of Consumer Personal Data Protection in Ecommerce from the Perspective of Law No. 27 of 2022." *Journal of World Science* 3, no. 3 (2024): 410–18. doi:10.58344/jws.v3i3.584.
- Annan, Alaikha. "Tinjauan Yuridis Perlindungan Data Pribadi Pada Sektor Kesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022." *Synergy: Jurnal Ilmiah Multidisiplin* 1, no. 04 (2024): 247–54.
- Arifin, Smsul. "Melindungi Privasi Di Era Digital: Mengatasi Kebocoran Data Rekam Medis Pasien COVID-19." *Jatim.Tribunnews.Com*, 2025. <https://jatim.tribunnews.com/2025/01/08/melindungi-privasi-di-era-digital-mengatasi-kebocoran-data-rekam-medis-pasien-covid-19>.
- Budiman, Arief, Muzakar Isa, and Siti Soekiswati. "Analisis Risiko Dan Tindakan Pencegahan Kebocoran Data Rekam Medis Elektronik Pasien Di RS P Surakarta." *Ranah Research: Journal of Multidisciplinary Research and Development* 7, no. 3 (2025): 2118–27.
- CNN. "Waspada, Data Pribadi Pasien Potensi Bocor Saat Konsultasi Telehealth." *Cnnindonesia.Com*, 2022. <https://www.cnnindonesia.com/teknologi/20220105182546-185-743027/waspada-data-pribadi-pasien-potensi-bocor-saat-konsultasi-telehealth>.
- Indriyani, Novita. "Analisis Aspek Keamanan Data Pada SIMARS Dalam Penerapan Rekam Medis Elektronik Di RSUP Prof. Dr. IGNG Ngoerah Denpasar," 2023.
- Kliwanto, and Chandra Hamdani Noor. "Pakar Nilai Respons Kemenkes Lambat Terkait Laporan Kebocoran Data." *Antaranews.Com*, 2021. <https://www.antaranews.com/berita/2365010/pakar-nilai-respons-kemenkes-lambat-terkait-laporan-kebocoran-data>.
- Mulyadita, Ulfathea, Edward Sutanto, Muhammad Fiqri, Ery Setiawan, and Anooj Pattnaik. "Mapping Telemedicine in Indonesia: Evidence for Policy Action at a Critical Juncture," 2025.
- Murima, Widya Hapsari, Ahmad Rido'i Yuda Prayogi, Aisyah Putri Rahvy, Nuranisah Djunaedi, and Inge Dhamanti. "Penggunaan Telemedicine Di Fasilitas Kesehatan Selama Pandemi Covid-19." *Indonesian Journal of Health Administration* 10, no. 2 (2022).
- Nurjanah, Lensa. "Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik Di Rumah Sakit Bethesda Yoyakarta," 2023.
- Putra, Calvin Anthony, and Muhammad Ali Masnun. "Analisis Pertanggungjawaban Rumah Sakit Terkait Potensi Kebocoran Data Rekam Medis Elektronik Akibat Cyber Crime." *Novum: Jurnal Hukum* 9, no. 2 (2022): 191–200.



-
- Sari, Rita Pusputa. "Telehealth Dan Telemedicine: Solusi Akses Kesehatan Digital." *Cloudcomputing.Id*, 2025. <https://www.cloudcomputing.id/berita/telehealth-solusi-kesehatan-digital>.
- Susanto, Edy, Adhani Windari, and Rizkiyatul Amalia. "EDIKASI: Empowering Data Integrity and Knowledge on Health Information Release in the Digital Era." *LINK* 20, no. 2 (2024): 113–17.
- Wiraguna, Sidi Ahyar. "Metode Normatif Dan Empiris Dalam Penelitian Hukum : Studi Eksploratif Di Indonesia" 3, no. 3 (2024). doi:10.59818/jps.v3i3.1390.