JK: Jurnal Kesehatan
Vol. 3 No. 2 Juli 2025, hal., 148-158
e-ISSN: 2987-9655

IMPLEMENTASI PERLINDUNGAN DATA PRIBADI PASIEN DALAM LAYANAN TELEMEDICINE DI INDONESIA: ANALISIS REGULASI DAN TANTANGAN PRAKTIS

Gunawan Widjaja
Senior Lecturer Faculty of Law Universitas 17 Agustus 1945 Jakarta
widjaja_gunawan@yahoo.com

Wagiman
Senior Lecturer Faculty of Law Universitas 17 Agustus 1945 Jakarta
wagimanmartedjo68@gmail.com

Dyah Ersita Yustanti
Senior Lecturer Faculty of Law Universitas 17 Agustus 1945 Jakarta
dyustanti@yahoo.com

Hotmaria Hertawaty Sijabat
Researcher, Faculty of Law Universitas 17 Agustus 1945 Jakarta
sijabathotmaria@gmail.com

Handojo Dhanudibroto
Doctoral Student, Faculty of Law Universitas 17 Agustus 1945 Jakarta
nonowang0603@gmail.com

Abstract

Digital transformation in Indonesia's health sector has accelerated the adoption of telemedicine services as an alternative to remote medical services, especially since the COVID-19 pandemic. Telemedicine provides easy access and efficiency of health services for the community, but at the same time increases challenges related to the protection of patients' personal data stored and processed digitally. This study employs a normative legal method with a literature review to analyse regulations governing the protection of patient personal data in telemedicine services in Indonesia, as well as to identify practical challenges in their implementation in the field. The results of the study indicate that although there is a fairly comprehensive legal basis, such as Law No. 27 of 2022 on Personal Data Protection and various other health sector regulations, implementation at the operational level still faces obstacles. These challenges include weak data security infrastructure, low digital literacy among medical personnel and patients, lack of specific technical guidelines, and limited oversight and enforcement of data protection violations. Collaborative efforts between the government, healthcare providers, and the public are needed to strengthen the personal data protection ecosystem, thereby ensuring safe, inclusive, and trustworthy telemedicine services in Indonesia.

***Keywords**: Personal Data Protection, Telemedicine, Health Law, Regulation, Indonesia.*

Abstrak

Transformasi digital di sektor kesehatan Indonesia telah mempercepat adopsi layanan telemedicine sebagai alternatif pelayanan medis jarak jauh, terutama sejak pandemi COVID-19. Telemedicine memberikan kemudahan akses dan efisiensi layanan kesehatan bagi masyarakat, namun sekaligus meningkatkan tantangan terkait perlindungan data pribadi pasien yang tersimpan dan diproses secara digital. Penelitian ini menggunakan metode yuridis normatif dengan kajian pustaka untuk menganalisis regulasi yang mengatur perlindungan data pribadi pasien dalam layanan telemedicine di Indonesia, serta mengidentifikasi tantangan praktis implementasinya di lapangan. Hasil studi menunjukkan bahwa walaupun telah terdapat landasan hukum yang cukup komprehensif, seperti Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dan berbagai peraturan sektor kesehatan lainnya, implementasi di tingkat operasional masih menghadapi kendala. Kendala tersebut meliputi lemahnya infrastruktur keamanan data, rendahnya literasi digital tenaga medis dan pasien, kurangnya pedoman teknis spesifik, serta terbatasnya pengawasan dan penegakan hukum terhadap pelanggaran perlindungan data. Diperlukan upaya kolaboratif antara pemerintah, penyedia layanan kesehatan, dan masyarakat untuk memperkuat ekosistem perlindungan data pribadi, demi terciptanya layanan telemedicine yang aman, inklusif, dan terpercaya di Indonesia.

Kata Kunci: Perlindungan Data Pribadi, Telemedicine, Hukum Kesehatan, Regulasi, Indonesia.

Pendahuluan

Transformasi digital di sektor kesehatan Indonesia telah mengalami perkembangan pesat dalam satu dekade terakhir, dipicu oleh kemajuan teknologi informasi dan komunikasi yang semakin merasuk ke seluruh aspek layanan medis. Telemedicine kemudian muncul sebagai inovasi utama yang menawarkan kemudahan konsultasi, diagnosis, dan penanganan pasien secara daring, menembus batasan geografis yang selama ini menjadi kendala utama distribusi layanan Kesehatan (Annan, 2024).

Luasnya wilayah Indonesia disertai tantangan geografis dan demografis telah menyulitkan pemerataan akses layanan kesehatan, terutama di wilayah tertinggal, terdepan, dan terluar. Kehadiran telemedicine menawarkan solusi efektif untuk mengatasi hambatan-hambatan ini dengan memperluas jangkauan layanan medis ke daerah-daerah yang belum memiliki fasilitas kesehatan yang memadai maupun jumlah tenaga medis yang terbatas (Rahma & Supriyadi, 2024).

Pemerintah Indonesia sejak tahun 2015 telah menerbitkan berbagai regulasi strategis seperti Peraturan Menteri Kesehatan dan Keputusan Menteri Kesehatan yang secara eksplisit mendukung penyelenggaraan telemedicine. Dukungan regulasi ini menegaskan komitmen pemerintah dalam mendorong pemanfaatan teknologi digital guna memberikan pelayanan kesehatan yang lebih merata dan dapat diakses oleh

seluruh lapisan Masyarakat (*Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*, 2022).

Pandemi COVID-19 yang melanda pada tahun 2020 menjadi momentum akselerasi adopsi telemedicine secara masif di Indonesia. Pembatasan mobilitas fisik serta lonjakan kebutuhan layanan kesehatan mendorong inovasi dalam pelaksanaan layanan medis melalui platform digital, sehingga telemedicine mengalami peningkatan pemanfaatan secara signifikan dan perannya menjadi vital dalam menjaga keberlangsungan sistem kesehatan nasional. Setelah pandemi, pola konsumsi layanan kesehatan masyarakat mengalami perubahan drastis. Masyarakat dan tenaga medis mulai terbiasa dengan konsultasi virtual dan telemedicine tidak lagi dianggap sebagai solusi alternatif semata, melainkan telah menjadi bagian dari sistem layanan kesehatan yang berkelanjutan dan terintegrasi dengan pola layanan tatap muka konvensional yang sudah ada (Rimbun et al., 2024).

Manfaat telemedicine dalam konteks Indonesia sangat nyata, mulai dari efisiensi waktu dan biaya, pengurangan kepadatan dan antrean di fasilitas kesehatan, hingga peningkatan akses masyarakat terhadap layanan medis, khususnya bagi masyarakat yang tinggal di daerah terpencil. Telemedicine adalah penyelenggaraan pelayanan kesehatan jarak jauh yang dilakukan oleh profesional kesehatan dengan memanfaatkan teknologi informasi dan komunikasi, sehingga memungkinkan pertukaran informasi diagnosis, pengobatan, pencegahan penyakit dan cedera, penelitian, evaluasi, serta pendidikan berkelanjutan tanpa keharusan hadir secara fisik di fasilitas medis (Yuliana, 2021). Tujuan utama telemedicine adalah meningkatkan aksesibilitas dan mutu layanan kesehatan, terutama bagi masyarakat yang tinggal di daerah terpencil atau kesulitan mengakses fasilitas kesehatan, dengan tetap menjaga standar pelayanan klinis dan kerahasiaan data pasien sesuai peraturan perundang-undangan yang berlaku (Pramukars, 2021).

Selain itu, telemedicine juga memungkinkan adanya pemantauan pasien secara kontinu, akses konsultasi spesialis lintas wilayah, serta peningkatan kapasitas tenaga kesehatan melalui pelatihan daring. Namun demikian, implementasi telemedicine menghadapi berbagai tantangan signifikan. Keterbatasan infrastruktur teknologi di sejumlah wilayah, masih rendahnya literasi digital di kalangan masyarakat dan tenaga kesehatan, serta adanya disparitas mutu layanan menjadi beberapa hambatan utama yang perlu diatasi agar manfaat telemedicine benar-benar merata dan optimal (Dalimunthe, 2024).

Di balik efisiensi dan kemudahan yang ditawarkan, telemedicine memunculkan permasalahan baru terkait privasi dan perlindungan data pribadi pasien. Proses pengumpulan, penyimpanan, hingga pengelolaan data medis elektronik menyimpan potensi kerentanan kebocoran data dan penyalahgunaan apabila tidak diatur dengan sistem pengamanan yang matang dan regulasi yang tegas (Putri Purnama, 2025). Untuk menjawab tantangan tersebut, pemerintah telah mengesahkan Undang-undang No. 27

Tahun 2022 tentang Perlindungan Data Pribadi yang secara khusus memberikan jaminan dan pengaturan mengenai perlindungan hak privasi warga negara, termasuk dalam konteks layanan telemedicine. Selain itu, regulasi pendukung lain seperti Undang-undang ITE, berbagai Permenkes tentang penyelenggaraan telemedicine dan rekam medis elektronik turut memperkuat landasan hukum terkait perlindungan data (*Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*, 2022, p. 27).

Meskipun kerangka hukum telah tersedia, sejumlah insiden kebocoran data pribadi di sektor kesehatan, seperti kasus e-HAC dan eksposur data pasien COVID-19, membuktikan bahwa perlindungan data kesehatan digital di Indonesia masih menghadapi banyak tantangan nyata di tingkat implementasi. Kejadian tersebut menjadi alarm penting untuk memprioritaskan penguatan standar keamanan data dan penerapan sanksi yang tegas bagi pihak-pihak yang lalai maupun melanggar regulasi (Nurhayati, 2025). Berbagai upaya penguatan implementasi perlindungan data pribadi sedang digalakkan melalui peningkatan literasi hukum, pelatihan keamanan digital bagi tenaga medis, serta monitoring berkala yang menyeluruh pada seluruh penyelenggara layanan kesehatan berbasis digital. Kolaborasi lintas sektor antara pemerintah, swasta, dan masyarakat memainkan peran penting dalam memastikan akuntabilitas perlindungan data pasien (Wahyudin, 2025).

Dalam konteks ini, penelitian hukum mengenai implementasi perlindungan data pribadi pasien pada layanan telemedicine menjadi sangat relevan dan krusial, agar perkembangan inovasi teknologi tidak mengabaikan perlindungan hak privasi maupun etika profesi kesehatan. Diperlukan analisis mendalam terkait regulasi yang berlaku serta identifikasi tantangan praktis di lapangan demi menghasilkan landasan kebijakan dan rekomendasi yang dapat memperkuat ekosistem layanan kesehatan digital di Indonesia ke depan (Syarifuddin, 2024).

Kajian ini mendukung upaya nyata mewujudkan sistem pelayanan kesehatan digital yang aman, inklusif, serta menghormati hak-hak pasien atas privasi dan perlindungan data pribadi. Dengan demikian, manfaat telemedicine dapat terdistribusi secara adil tanpa mengorbankan prinsip etika, keamanan, dan kepercayaan masyarakat terhadap layanan kesehatan berbasis teknologi.

Metode Penelitian

Metode penelitian yang digunakan adalah metode yuridis normatif berbasis kajian pustaka, yaitu penelitian hukum yang memfokuskan kajian pada bahan hukum primer dan sekunder yang relevan dengan perlindungan data pribadi pasien dalam layanan telemedicine di Indonesia. Pengumpulan data dilakukan melalui studi literatur terhadap undang-undang, peraturan pemerintah, peraturan menteri kesehatan, serta dokumen-dokumen hukum, jurnal, dan artikel ilmiah yang membahas telemedicine dan perlindungan data pribadi (Eliyah & Aslan, 2025). Pendekatan yang dipakai mencakup statute approach untuk menganalisis norma hukum positif yang berlaku dan conceptual

approach dengan membandingkan prinsip-prinsip perlindungan data internasional, sedangkan analisis data dilakukan secara deskriptif kualitatif dengan menguraikan, membandingkan, dan menafsirkan ketentuan hukum untuk mengidentifikasi celah regulasi dan tantangan implementasi di lapangan (Bolderston, 2008).

Hasil dan Pembahasan

Analisis Regulasi Perlindungan Data Pribadi Pasien dalam Telemedicine

Pertumbuhan telemedicine di Indonesia telah menghadirkan kemudahan akses layanan kesehatan, terutama bagi masyarakat yang tinggal di wilayah terpencil maupun daerah dengan keterbatasan fasilitas kesehatan. Dalam praktiknya, layanan telemedicine memungkinkan pasien dan tenaga medis melakukan konsultasi, diagnosis, serta perawatan secara daring melalui beragam aplikasi berbasis teknologi informasi, yang secara langsung berimplikasi pada pengumpulan dan pengelolaan data pribadi pasien secara digital (Lestari, 2020).

Konsekuensi dari digitalisasi pelayanan kesehatan ini adalah meningkatnya risiko terhadap privasi pasien. Data pribadi pasien tidak lagi sekadar tercatat secara fisik di fasilitas kesehatan, melainkan tersimpan dan dipertukarkan secara daring. Hal ini menuntut adanya perlindungan hukum yang jelas demi menjaga keamanan data dan mencegah penyalahgunaan informasi sensitif pasien, seperti riwayat penyakit, hasil pemeriksaan laboratorium, dan data identitas pribadi (Yusriadi, 2025).

Pemerintah Indonesia telah mengatur perlindungan data pribadi pasien melalui sejumlah regulasi. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi dasar utama pengaturan perlindungan data pribadi di era digital, termasuk untuk data kesehatan pasien telemedicine (*Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*, 2022). Selain UU PDP, terdapat juga Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan yang memberikan landasan perlindungan hak pasien, serta Peraturan Menteri Kesehatan No. 20 Tahun 2019 yang secara khusus mengatur penyelenggaraan telemedicine antar fasilitas pelayanan Kesehatan.

UU PDP secara tegas mengklasifikasikan data kesehatan sebagai data pribadi yang bersifat spesifik. Pasal-pasal dalam UU ini mewajibkan pengendali data, termasuk penyedia layanan telemedicine, untuk senantiasa menjaga kerahasiaan dan keamanan data pribadi sepanjang proses pengumpulan, penyimpanan, pemrosesan, maupun penghapusan data. Dalam praktik telemedicine, ketentuan ini mengharuskan adanya persetujuan eksplisit dari pasien sebelum data pribadi mereka dikumpulkan atau dibagikan kepada pihak ketiga (Purnama, 2024).

Perlindungan data pribadi pasien juga diatur dalam Permenkes No. 20 Tahun 2019, yang mengharuskan pelayanan telemedicine dilakukan antar fasilitas kesehatan dengan memenuhi standar keamanan sistem elektronik. Penyedia layanan wajib menerapkan enkripsi, autentikasi, dan sistem pengamanan lainnya guna mencegah

akses ilegal, perubahan, maupun kebocoran data pasien selama proses transmisi informasi medis (*Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*, 2022, p. 20).

Kendati demikian, harmonisasi antara berbagai regulasi yang mengatur perlindungan data pasien dinilai masih belum optimal. Ketidakjelasan mengenai tata laksana teknis pengelolaan data pada level aplikasi telemedicine dan perbedaan ruang lingkup fokus antara UU Kesehatan, Permenkes, serta UU PDP kerap memicu kebingungan dalam menentukan standar kepatuhan yang harus ditaati oleh penyedia layanan digital. Salah satu celah krusial adalah absennya pengaturan khusus terhadap telemedicine berbasis aplikasi komersial yang melayani konsultasi langsung antara pasien dan dokter di luar sistem rumah sakit (Bonsapia & Jumiran, 2025). Sementara Permenkes 20/2019 lebih banyak mengatur telemedicine antar fasilitas kesehatan, UU PDP menetapkan standar privasi yang ketat namun belum memiliki pedoman praktis khusus untuk sektor kesehatan digital. Hal ini menyebabkan ketidakharmonisan dan ketidaktahuan penyedia aplikasi dalam mematuhi standar perlindungan data yang seharusnya berlaku (Nadiroh & Wiraguna, 2025).

Dalam implementasinya, masalah utama terjadi pada aspek penegakan hukum dan keterbatasan pengawasan. Meskipun UU PDP memiliki pasal-pasal yang memuat ketentuan sanksi administratif maupun pidana atas pelanggaran terhadap data pribadi, mekanisme monitoring dan penegakannya masih menghadapi tantangan, khususnya dalam lingkungan digital yang dinamis dan melibatkan banyak pihak lintas batas yurisdiksi (Purwanto, 2025).

Praktik keamanan data digital sendiri masih lemah di sejumlah penyelenggara telemedicine. Kasus kebocoran data pasien—seperti yang terjadi pada aplikasi e-HAC dan insiden eksposur hasil tes COVID-19—menjadi contoh nyata lemahnya sistem pengamanan, baik dari sisi teknologi maupun dari sisi komitmen manajemen. Selain akibat kekurangan sistem enkripsi data, banyak penyedia layanan juga belum menjalankan audit data maupun pelatihan keamanan siber secara berkala. Keterbatasan infrastruktur dan kesenjangan literasi digital turut memperparah tantangan perlindungan data. Tenaga kesehatan dan pasien di daerah non-perkotaan seringkali belum memahami pentingnya prinsip privasi dan tata kelola data digital yang baik, sehingga kerap mengabaikan prosedur keamanan seperti penggunaan kata sandi kuat, verifikasi dua faktor, hingga pembaruan perangkat lunak keamanan (Fadilah & Saragih, 2022).

Selain itu, tantangan lain yang tidak kalah serius adalah resistensi dari penyelenggara layanan kesehatan yang masih menganggap regulasi perlindungan data sebagai beban administratif semata. Kurangnya investasi pada sistem keamanan siber dan minimnya pelatihan keamanan data di fasilitas kesehatan menimbulkan risiko berkelanjutan dalam praktik telemedicine (Annan, 2024). Kedisiplinan penyedia layanan dalam mengantongi informed consent dari pasien patut mendapat perhatian khusus.

Banyak aplikasi telemedicine masih menggunakan format persetujuan yang tidak jelas, atau menggabungkan persetujuan penggunaan data dengan syarat dan ketentuan layanan, sehingga tidak benar-benar memenuhi prinsip transparansi dan kebebasan memilih dari pasien (Rahma & Supriyadi, 2024).

Di sisi lain, kurangnya sanksi tegas serta masih lemahnya pengawasan dari otoritas berwenang menyebabkan pelanggaran privasi kerap kali tidak ditindaklanjuti secara efektif. Meski UU PDP mewajibkan pelaporan insiden pelanggaran data pribadi, dalam praktiknya mekanisme ini jarang diimplementasikan secara terbuka oleh penyedia layanan, dan seringkali publik baru mengetahui adanya kebocoran data setelah kasus menjadi viral di media (Rimbun et al., 2024). Beberapa upaya telah dilakukan untuk meningkatkan kapasitas perlindungan data pasien, termasuk program sosialisasi, pelatihan keamanan digital, serta peningkatan standar infrastruktur dan teknologi pada layanan telemedicine. Pemerintah juga mendorong kolaborasi lintas sektor antara regulator, penyedia layanan, dan masyarakat guna memperkuat akuntabilitas dan membangun ekosistem keamanan data yang lebih transparan (Yuliana, 2021).

Namun demikian, hasil analisis menunjukkan bahwa kerangka hukum yang ada, meski sudah relatif lengkap secara normatif, masih memerlukan harmonisasi dan penyesuaian, terutama dalam menjawab tantangan praktik telemedicine yang sangat cepat berkembang. Regulasi perlu merespons dinamika teknologi baru dan kebiasaan masyarakat digital agar mampu melindungi hak-hak pasien secara efektif dan berkelanjutan.

Penegakan prinsip-prinsip perlindungan data internasional seperti lawfulness, fairness, dan transparency juga perlu dipertegas dalam pedoman teknis sektor kesehatan digital. Hal ini penting untuk membangun kepercayaan masyarakat, mengingat sensitivitas data medis sangat tinggi dan sering menjadi target serangan siber maupun penyalahgunaan oleh pihak tidak bertanggung jawab (Pramukars, 2021).

Dengan demikian, melalui analisis regulasi dan tantangan praktik yang dihadapi, tampak bahwa perlindungan data pribadi pasien dalam layanan telemedicine memerlukan pendekatan yang terpadu dan adaptif. Kolaborasi antara legislator, penegak hukum, penyedia layanan, serta literasi pasien menjadi syarat mutlak untuk membangun sistem kesehatan digital yang aman, inklusif, dan berorientasi pada perlindungan hak-hak pasien di masa depan.

Tantangan Praktis Dalam Penerapan Perlindungan Data Pribadi Pasien

Implementasi perlindungan data pribadi pasien dalam layanan telemedicine di Indonesia menghadapi serangkaian tantangan praktis yang kompleks. Salah satu tantangan utama adalah rendahnya tingkat kesadaran dan pemahaman para tenaga medis serta penyelenggara layanan digital terkait pentingnya pelindungan data pribadi pasien. Meskipun regulasi telah mendorong perlindungan data, masih banyak penyedia

layanan yang belum memahami konsep dasar keamanan siber dan privasi, sehingga menimbulkan praktik lemah dalam pengelolaan data sensitive (*Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*, 2022).

Penyebab lain yang sangat krusial adalah lemahnya infrastruktur teknologi di berbagai fasilitas kesehatan, terutama di wilayah tertinggal. Banyak institusi kesehatan yang belum memiliki sistem penyimpanan dan keamanan data yang memadai. Kondisi ini memperbesar risiko terjadinya akses ilegal, peretasan, maupun kehilangan data pasien, mengingat data sering disimpan secara terpusat tanpa sistem cadangan dan enkripsi yang layak (Annan, 2024). Ketidakmerataan sumber daya manusia (SDM) menjadi tantangan signifikan. Sebagian fasilitas kesehatan, terutama di daerah, masih kekurangan staf IT berkompeten yang fokus pada keamanan data dan pelatihan tenaga medis di bidang perlindungan data masih terbatas. Padahal, kompetensi SDM sangat berpengaruh pada efektivitas penerapan sistem perlindungan data pribadi.

Biaya investasi yang tinggi untuk membangun infrastruktur keamanan siber juga menjadi penghambat implementasi perlindungan data secara optimal. Fasilitas kesehatan dengan anggaran terbatas cenderung menunda pembaruan sistem dan perangkat lunak keamanan, sehingga semakin rentan terhadap serangan siber dan insiden kebocoran data. Fragmentasi dan integrasi sistem data kesehatan di Indonesia turut memperbesar kerentanan. Banyaknya aplikasi kesehatan yang dikembangkan pemerintah dan swasta tanpa standardisasi mengakibatkan pertukaran data yang tidak efisien serta kontrol keamanan yang lemah. Fragmentasi ini berkontribusi terhadap inkonsistensi penerapan kebijakan perlindungan data di berbagai platform (Rahma & Supriyadi, 2024).

Kepatuhan terhadap regulasi hukum seperti UU PDP, Permenkes tentang telemedicine, dan rekam medis elektronik kerap tidak berjalan optimal di lapangan. Sebagian besar penyedia layanan, khususnya platform komersial, masih mengalami kebingungan akibat belum adanya pedoman teknis yang spesifik dari pemerintah mengenai cara implementasi standar perlindungan data di layanan telemedicine. Masalah selanjutnya adalah lemahnya monitoring dan penegakan hukum. Banyak kasus pelanggaran data, seperti kebocoran data eHAC dan BPJS Kesehatan, berakhir tanpa sanksi tegas maupun penyelesaian tuntas. Hal ini menurunkan efek jera bagi pelaku dan kepercayaan publik terhadap sistem keamanan digital sektor Kesehatan (Rimbun et al., 2024).

Persetujuan eksplisit (informed consent) pasien juga kerap dicapai secara formalitas semata. Masih banyak aplikasi yang menggunakan persetujuan data secara agregat dalam "syarat dan ketentuan" tanpa memastikan pasien memahami konsekuensinya, sehingga berpotensi melanggar prinsip transparansi dan akuntabilitas. Keterbatasan pelatihan keamanan digital bagi tenaga medis dan staf administrasi menambah daftar tantangan. Banyak tenaga kesehatan belum dibekali sosialisasi maupun literasi memadai mengenai prosedur keamanan data, seperti penggunaan kata

sandi kuat, autentikasi dua faktor, dan kewaspadaan atas ancaman phising atau malware (Yuliana, 2021).

Pengelolaan privasi data pasien juga diperburuk oleh praktik penggunaan aplikasi umum (seperti WhatsApp dan Zoom) untuk konsultasi medis, bukan aplikasi telemedicine yang teregistrasi dan dilengkapi fitur keamanan standar. Penggunaan saluran komunikasi yang tidak aman ini meningkatkan risiko penyadapan dan akses ilegal terhadap data medis sensitif. Rendahnya kepedulian masyarakat tentang hak dan kewajiban pengelolaan data turut menjadi tantangan. Banyak pasien belum memahami hak mereka untuk mengatur, mengoreksi, atau menuntut penghapusan data pribadi, sehingga kurang proaktif dalam melaporkan pelanggaran atau insiden kebocoran data (Pramukars, 2021).

Penyalahgunaan data oleh pihak internal juga tidak dapat diabaikan. Riset menunjukkan, sejumlah kasus pelanggaran data pasien disebabkan oleh pegawai atau mitra kerja yang tidak bertanggung jawab, baik karena lalai maupun motif criminal. Ini menandakan perlunya audit rutin dan pengawasan internal yang lebih ketat terhadap akses data. Serangan siber seperti ransomware, phising, dan malware semakin sering menyasar institusi kesehatan. Serangan ini bukan hanya mengakibatkan kerugian finansial, tapi juga dapat mengancam keselamatan pasien jika data medis vital hilang atau diacak (Dalimunthe, 2024). Kurangnya audit dan mekanisme penilaian risiko secara berkala menyebabkan banyak kerentanan keamanan sistem tidak teridentifikasi dan ditangani dengan tepat waktu. Layanan digital kesehatan yang tidak melakukan audit keamanan cenderung memiliki standar perlindungan data yang lemah. Keterlibatan pihak ketiga, seperti vendor teknologi atau cloud provider, juga membawa risiko tambahan. Banyak pengelola data yang tidak mengevaluasi kecukupan kontrol keamanan vendor, sehingga memungkinkan akses oleh pihak eksternal yang tidak diinginkan (Purnama, 2024).

Dampak dari tantangan-tantangan tersebut sangat nyata, salah satunya penurunan kepercayaan masyarakat terhadap layanan telemedicine akibat kekhawatiran data medis mereka disalahgunakan atau bocor ke publik. Kepercayaan yang rendah pada sistem digital secara langsung memperlambat adopsi dan optimalisasi telemedicine di Indonesia.

Keseluruhan tantangan di atas menunjukkan bahwa perlindungan data pribadi pasien di layanan telemedicine membutuhkan solusi menyeluruh, mulai dari investasi infrastruktur, pelatihan SDM, penyusunan pedoman teknis, harmonisasi regulasi, hingga penguatan penegakan hukum. Tanpa respons sistemik dan kolaborasi lintas sektor, perlindungan data dalam telemedicine sulit terwujud secara konsisten dan berkelanjutan.

Kesimpulan

Implementasi perlindungan data pribadi pasien dalam layanan telemedicine di Indonesia telah memiliki landasan hukum yang cukup komprehensif melalui Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan berbagai regulasi sektor kesehatan. Regulasi ini mewajibkan pengendali data, termasuk penyedia layanan telemedicine, untuk menjaga kerahasiaan, keamanan, serta memperoleh persetujuan yang transparan sebelum memproses data pasien. Upaya regulasi semacam ini berkontribusi dalam memperkuat kepercayaan masyarakat dan memberikan kepastian hukum atas pengelolaan data pribadi pasien di era layanan kesehatan digital.

Namun, di tingkat implementasi, masih ditemukan tantangan signifikan seperti lemahnya infrastruktur keamanan data, rendahnya literasi digital tenaga kesehatan dan pasien, kurangnya audit serta pengawasan rutin, serta fragmentasi standar teknis di antara penyelenggara layanan telemedicine. Belum meratanya pemahaman penyedia layanan tentang tata kelola data, serta ketidakhadiran pedoman teknis yang spesifik dari pemerintah, sering kali menyebabkan kepatuhan terhadap UU PDP berjalan tidak optimal. Sejumlah insiden kebocoran data pasien membuktikan bahwa perlindungan data di sektor ini masih perlu penguatan nyata.

Oleh karena itu, perlindungan data pribadi pasien dalam telemedicine idealnya membutuhkan respons sistemik dengan memperkuat infrastruktur, meningkatkan edukasi dan pelatihan semua pihak, serta mendorong harmonisasi regulasi dan peningkatan kapasitas pengawasan. Kolaborasi antara pemerintah, institusi kesehatan, penyedia teknologi, dan masyarakat sangat esensial agar inovasi di bidang telemedicine tetap berjalan selaras dengan perlindungan hak privasi dan rasa aman bagi setiap pasien Indonesia.

References

Annan, A. (2024). Tinjauan Yuridis Perlindungan Data Pribadi pada Sektor Kesehatan Berdasarkan UU No. 27 Tahun 2022. *Synergy: Jurnal Ilmiah Multidisiplin*, *1*(4), 247–254.

Bolderston, A. (2008). Writing an Effective Literature Review. *Journal of Medical Imaging and Radiation Sciences*, 71–76.

Bonsapia, M. & Jumiran. (2025). Aspek Hukum Telemedicine di Indonesia. *The Juris*, *9*(1), 259–268. https://doi.org/10.56301/juris.v9i1.1636

Dalimunthe, W. (2024). Patient Legal Protection in the Digital Era and Study of Indonesian Telemedicine Regulation. *Jurnal Hukum Kesehatan Indonesia*, *1*(1), 1–10.

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

Fadilah & Saragih. (2022). Analisis Regulasi Telemedicine di Indonesia. *Jurnal Hukum & Kesehatan*, *5*(1).

Lestari, H. (2020). *Hukum Jaminan Kesehatan Nasional*. Pustaka Pelajar.

Nadiroh, A., & Wiraguna, S. A. (2025). Analisis Yuridis Kebocoran Data di Layanan Kesehatan Digital: Studi Kasus Aplikasi Telemedicine di Indonesia. *Media Hukum Indonesia*, *2*(6), 313–320.

Nurhayati, R. H. (2025). Legal Protection for Patients in Telemedic Services in Indonesia. *Journal of Legal, Public and Humanity*, *5*(3). https://doi.org/10.38035/jlph.v5i3.1592

Pramukars, D. T. (2021). Perlindungan Hukum bagi Pasien dalam Telemedicine. *Jurnal Cakrawala Informasi*, *1*(2), 51–56.

Purnama, S. (2024). Assessing Telemedicine Demand and Viability in Indonesian Geriatric Clinics: A Comprehensive HOT FIT and Sociotechnical Analysis. *Current Aging Science*, *18*(1), 47–58. https://doi.org/10.2174/0118746098302999240522092726

Purwanto, R. (2025). Analisis Regulasi Telemedicine di Indonesia. *Jurnal Innovation Research and Knowledge*, *5*(1).

Putri Purnama, N. N. (2025). Patient Data Privacy Challenges in Electronic Health Systems: A Juridical Analysis of Medical Information Protection in Indonesia. *West Science Law and Human Rights*, *3*(1), 1–8. https://doi.org/10.58812/wslhr.v3i01.1577

Rahma, D., & Supriyadi, H. (2024). Telemedicine Regulation in Indonesia: Legal Frameworks, Challenges, and Future Directions. *Journal of Law and Technology*, *7*(3), 213–230. https://doi.org/10.33560/jmiki.v13i1.795

Rimbun, L. R., Marisi, E. L. D. D., & Hidayati, T. (2024). Tantangan Keamanan Data dalam Telemedicine: Implikasi terhadap Privasi Pasien dan Kepercayaan dalam Layanan Kesehatan Digital: Systematic Review. *Malahayati Health Student Journal*, *4*(10).

Syarifuddin, A. (2024). Indonesian Telemedicine: Between Hope and Legal Challenges. *Indonesian Journal of Humanities and Social Sciences*, *5*(3), 1249–1258. https://doi.org/10.33367/ijhass.v5i3.5936

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. (2022).

Wahyudin, B. (2025). Legal Protection for Doctors in Telemedicine Services: Government Responsibility in Supporting SDGs 3 and 9 in Indonesia. *Journal of Lifestyle and SDGs Review*, *5*(3). https://doi.org/10.47172/2965-730X.SDGsReview.v5.n03.pe05139

Yuliana, D. (2021). *Tanggung Jawab Penyedia Layanan Kesehatan dalam Era Digitalisasi*.

Yusriadi, -. (2025). *Digital Transformation of Health Services in Indonesia Through the Utilization of AI, Big Data, and Telemedicine*. *5*(1), 85–93. https://doi.org/10.62951/icistech.v5i1.270