Jejakdigital
JURNAL ILMIAH MULTIDISIPLIN
Available online at https://indojurnal.com/index.php/jejakdigital

eISSN 3089-7734; pISSN 3089-7742
Vol. 2, No. 1, Tahun 2026
doi.org/10.63822/89y5sj86
Hal. 423-430

Pertanggungjawaban Pidana Tenaga Kesehatan Pada Pelanggaran Keamanan Data Pasien Di Era Telemedis : Analisis UU No. 17 Tahun 2023 Tentang Kesehatan

Andi Ervin Novara Jaya[1], Gusti Ayu Utami [2]
Program Studi Ilmu Hukum Fakultas Hukum Universitas Universitas Musamus Merauke[1,2]

*Email andiervin@unmus.ac.id; gustiayu@unmus.ac.id

Sejarah Artikel:

Diterima 04-12-2025
Disetujui 14-12-2025
Diterbitkan 16-12-2025

ABSTRACT

The development of digital technology has revolutionized health service systems in many countries, including Indonesia, through the implementation of telemedicine as part of the national digital transformation agenda. Telemedicine enhances accessibility, improves service efficiency, and expands the reach of healthcare services, particularly for communities in remote regions. However, the use of digital systems in medical services also introduces serious risks concerning the security and confidentiality of highly sensitive patient data. Electronic medical records, diagnostic results, and patients' personal information are now transmitted through electronic networks that may become targets of cyberattacks, data breaches, internal misuse, or vulnerabilities within application security systems. This study aims to analyze the criminal liability of healthcare professionals in cases of patient data breaches within telemedicine services. The research employs a normative legal method using statutory, conceptual, and comparative approaches supported by academic literature. The primary regulations examined include Law No. 17 of 2023 on Health, Law No. 27 of 2022 on Personal Data Protection (PDP), and relevant provisions of the Indonesian Criminal Code (KUHP) concerning violations of information confidentiality. The findings indicate that healthcare professionals may be held criminally liable if a data breach occurs due to intentional misconduct, gross negligence, or actions contrary to professional standards. However, within the modern telemedicine ecosystem, liability does not rest solely on individual healthcare providers; it also extends to healthcare facilities, digital platform providers, server operators, and third parties involved in data processing. This study emphasizes the need to update legal frameworks regarding the distribution of responsibilities, strengthen digital security standards, and harmonize policies between the health sector and the national cybersecurity sector.

Keywords: *Telemedicine, Patient Data, Criminal Liability, Health Law, Personal Data Protection*

ABSTRAK

Perkembangan teknologi digital telah merevolusi sistem pelayanan kesehatan di berbagai negara, termasuk Indonesia, melalui implementasi telemedis sebagai bagian dari transformasi digital nasional. Telemedis memberikan kemudahan akses, efisiensi layanan, dan memperluas jangkauan pelayanan kesehatan bagi masyarakat di wilayah terpencil. Namun, penggunaan sistem digital dalam layanan medis juga memunculkan risiko serius terkait keamanan dan kerahasiaan data pasien yang bersifat sangat sensitif. Data rekam medis, hasil pemeriksaan, maupun informasi identitas pasien kini berpindah melalui jaringan elektronik yang dapat menjadi sasaran serangan siber, kebocoran data, penyalahgunaan internal, maupun kelemahan sistem keamanan aplikasi.Studi ini bertujuan menganalisis pertanggungjawaban pidana tenaga kesehatan dalam kasus kebocoran data pasien pada layanan telemedis. Penelitian dilakukan

dengan metode hukum normatif menggunakan pendekatan perundang-undangan, konseptual, serta perbandingan literatur akademik. Regulasi utama yang dianalisis mencakup UU No. 17 Tahun 2023 tentang Kesehatan, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP), serta ketentuan dalam KUHP terkait pelanggaran kerahasiaan informasi. Hasil penelitian menunjukkan bahwa tenaga kesehatan dapat dimintai pertanggungjawaban pidana apabila kebocoran data terjadi karena unsur kesengajaan, kelalaian berat, atau tindakan yang bertentangan dengan standar profesi. Namun, dalam ekosistem telemedis modern, tanggung jawab tidak hanya berada pada tenaga kesehatan individu, tetapi juga melibatkan fasilitas kesehatan, penyedia aplikasi digital, pemilik server, dan pihak ketiga yang terlibat dalam pemrosesan data. Penelitian ini menegaskan perlunya pembaruan pengaturan hukum mengenai pembagian tanggung jawab, peningkatan standar keamanan digital, serta harmonisasi kebijakan antara sektor kesehatan dan sektor keamanan siber nasional.

Kata Kunci: Telemedis, Data Pasien, Pertanggungjawaban Pidana, Hukum Kesehatan, Perlindungan Data Pribadi.

Bagaimana Cara Sitasi Artikel ini:

Andi Ervin Novara Jaya, & Gusti Ayu Utami. (2025). Pertanggungjawaban Pidana Tenaga Kesehatan Pada Pelanggaran Keamanan Data Pasien Di Era Telemedis : Analisis UU No. 17 Tahun 2023 Tentang Kesehatan. Jejak Digital: Jurnal Ilmiah Multidisiplin, 2(1), 423-430. https://doi.org/10.63822/89y5sj86

PENDAHULUAN

Pemanfaatan teknologi digital dalam dunia kesehatan telah mengalami akselerasi signifikan, terutama sejak terjadinya pandemi COVID-19 yang memaksa layanan kesehatan beradaptasi terhadap pembatasan mobilitas. Telemedis muncul sebagai bentuk inovasi layanan kesehatan yang memungkinkan interaksi antara tenaga kesehatan dan pasien tanpa tatap muka, melalui media elektronik seperti aplikasi, video call, platform kesehatan digital, maupun sistem rekam medis elektronik (RME). Transformasi ini menciptakan paradigma baru dalam pelayanan kesehatan yang jauh lebih efisien, cepat, dan dapat menjangkau masyarakat yang sebelumnya sulit memperoleh layanan kesehatan konvensional, termasuk masyarakat pesisir, kepulauan, dan daerah 3T.

Namun, perkembangan ini juga memunculkan tantangan besar, terutama terkait keamanan data pasien. Rekam medis merupakan data pribadi yang tergolong sangat sensitif, sebagaimana ditegaskan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan. Kedua regulasi tersebut mewajibkan penyelenggara pelayanan kesehatan dan tenaga kesehatan untuk menjaga kerahasiaan, integritas, dan keamanan data pasien. Pelanggaran terhadap kewajiban ini dapat menimbulkan konsekuensi pidana, perdata, dan administratif.

Risiko kebocoran data dalam telemedis dapat terjadi pada berbagai tahap: proses input data, penyimpanan, transmisi melalui jaringan internet, hingga akses oleh pihak internal fasilitas kesehatan. Banyak kasus kebocoran data kesehatan di Indonesia terjadi akibat kombinasi kelalaian manusia, lemahnya sistem keamanan digital, serangan siber, dan tidak diterapkannya standar keamanan yang memadai. Di sisi lain, regulasi mengenai pembagian tanggung jawab pidana antara tenaga kesehatan, fasilitas kesehatan, dan penyedia aplikasi telemedis belum diatur secara detail.

Oleh karena itu, penelitian ini penting untuk memberikan analisis komprehensif terkait bagaimana konsep pertanggungjawaban pidana diterapkan dalam konteks kebocoran data pasien pada era telemedis. Kajian ini tidak hanya menekankan pada unsur kesalahan tenaga kesehatan tetapi juga pada aspek kelembagaan, teknologi, dan tata kelola digital kesehatan.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang undangan dan pendekatan konseptual.sumber data terdiri dari peraturan perundang undangan,doktrin hukum pidana,buku, serta literatur mengenai telemedis dan keamanan data kesehatan.seluruh bahan hukum dianalisis menggunakan analisis kualitatif untuk memperoleh argumentasi hukum yang sistematis dan mengkaji keseuaian norma hukum pidana

HASIL DAN PEMBAHASAN

Landasan Hukum Perlindungan Data Pasien Dalam telemedis

Perlindungan data pasien dalam telemedis merupakan aspek fundamental yang menuntut perhatian serius dari tenaga kesehatan, penyelenggara layanan kesehatan, serta pemerintah sebagai regulator. UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menetapkan data kesehatan sebagai kategori data pribadi spesifik yang mendapat perlindungan hukum tingkat tinggi. Ketentuan ini bertujuan untuk memastikan bahwa setiap informasi yang berhubungan dengan keadaan fisik, mental, riwayat

penyakit, serta hasil pemeriksaan medis dilindungi dari potensi penyalahgunaan. Selain itu, UU Kesehatan Nomor 17 Tahun 2023 secara eksplisit mewajibkan seluruh tenaga kesehatan untuk menjaga kerahasiaan rekam medis pasien. Pelanggaran terhadap ketentuan ini tidak hanya bersifat administratif atau etis, tetapi juga dapat berimplikasi pada pertanggungjawaban pidana apabila unsur-unsur kesalahan terpenuhi. Dalam praktik telemedis, rekam medis dan data pasien dipertukarkan secara elektronik, sehingga risiko serangan siber dan kebocoran data meningkat signifikan. Kebocoran ini dapat terjadi melalui peretasan, penyimpanan data yang tidak aman, minimnya penerapan enkripsi, hingga kelalaian penggunaan perangkat digital oleh tenaga kesehatan. Oleh karena itu, kerangka hukum yang mengatur perlindungan data pasien harus dipahami secara komprehensif, termasuk ketentuan akses tanpa hak, penyebaran informasi, serta pemanfaatan data yang melampaui tujuan pelayanan kesehatan. Konteks digitalisasi yang masif menuntut adanya reformasi, harmonisasi, dan penegakan aturan yang kuat agar perlindungan hukum terhadap data pasien tidak hanya bersifat normatif tetapi juga efektif dalam implementasinya.

Klasifikasi Pelanggaran Keamanan Data oleh Tenaga Kesehatan

Pelanggaran keamanan data pasien dalam ekosistem telemedis memiliki spektrum yang luas dan dapat diklasifikasikan berdasarkan sifat pelanggarannya, tingkat kesalahan pelaku, serta mekanisme terjadinya insiden. Pada tingkat paling dasar, pelanggaran seringkali berasal dari kelalaian ringan (minor negligence) seperti penggunaan jaringan internet publik untuk mengakses rekam medis, tidak mengaktifkan pengunci layar perangkat, atau tidak memperbarui perangkat lunak keamanan. Walaupun terlihat sederhana, kelalaian ini dapat membuka titik masuk bagi pelaku siber untuk menyusup ke sistem.

Bentuk berikutnya adalah kelalaian berat (gross negligence) yang terjadi ketika tenaga kesehatan mengabaikan prosedur operasional standar terkait kerahasiaan data. Contoh umum termasuk mengunduh data pasien ke perangkat pribadi tanpa enkripsi, membagikan hasil konsultasi pasien melalui aplikasi pesan instan non-resmi, atau menyimpan data dalam aplikasi cloud yang tidak tersertifikasi keamanan. Kelalaian berat ini sering menjadi penyebab terbesar kebocoran data dalam layanan kesehatan digital.

Selain kelalaian, terdapat pelanggaran internal yang disengaja (intentional insider misconduct). Pelanggaran ini dilakukan oleh tenaga kesehatan atau staf internal yang memiliki akses sah ke sistem namun menyalahgunakannya untuk kepentingan pribadi, politik, atau ekonomi. Studi-studi global menunjukkan bahwa insiden kebocoran data paling sulit dideteksi justru berasal dari pelaku internal karena mereka sudah memahami struktur sistem.

Kategori lain adalah serangan eksternal (external cyberattacks) yang memanfaatkan kelemahan infrastruktur digital rumah sakit atau platform telemedis. Serangan dapat berupa phishing, ransomware, DDoS (Distributed Denial of Service), botnet, hingga pencurian identitas digital. Pelaku biasanya memanfaatkan kelalaian manusia sebagai pintu masuk, sehingga literasi digital tenaga kesehatan menjadi faktor penting.

Terakhir, terdapat pelanggaran sistemik (systemic breach) yang tidak terkait dengan individu, melainkan kelemahan menyeluruh pada desain sistem digital. Pelanggaran ini dapat terjadi apabila server tidak memiliki firewall memadai, tidak dilakukan audit keamanan rutin, atau sistem menggunakan perangkat lunak tidak berlisensi. Pelanggaran sistemik tergolong paling berbahaya karena dapat berdampak luas dan mempengaruhi ribuan data pasien sekaligus.

Klasifikasi ini menunjukkan bahwa ancaman kebocoran data tidak hanya terkait teknologi, tetapi juga perilaku manusianya. Karena itu, pendekatan pencegahan harus menggabungkan aspek teknologi, regulasi, dan pendidikan digital bagi seluruh tenaga kesehatan.

Pertanggungjawaban Pidana Tenaga Kesehatan

Pertanggungjawaban pidana tenaga kesehatan dalam kasus kebocoran data pasien berbasis telemedis harus dianalisis melalui dua unsur pokok, yaitu actus reus (perbuatan pidana) dan mens rea (kesalahan pelaku). Dalam praktiknya, UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah memberikan dasar hukum yang jelas bahwa setiap pihak yang memproses data pribadi wajib menjaga kerahasiaan dan integritasnya. Pelanggaran terhadap kewajiban tersebut dapat berimplikasi pada sanksi pidana jika terbukti terdapat unsur kesengajaan atau kelalaian berat.

Jika tenaga kesehatan secara aktif mengungkapkan atau menyebarkan data pasien tanpa hak, tindakan tersebut memenuhi unsur kesengajaan (dolus). Dalam hal ini, tenaga kesehatan dapat dikenai sanksi pidana berupa penjara dan denda sesuai ketentuan UU PDP. Namun, dalam kasus telemedis, unsur kelalaian lebih sering menjadi pemicu kebocoran data. Misalnya, tenaga kesehatan yang tidak mengikuti prosedur keamanan digital atau ceroboh dalam mengelola perangkat elektronik dapat dianggap melakukan kealpaan yang merugikan pasien.

Selain pertanggungjawaban individu, hukum pidana Indonesia juga memungkinkan pertanggungjawaban pidana korporasi (corporate criminal liability). Dalam konteks telemedis, korporasi dapat berupa rumah sakit, klinik, penyedia aplikasi telemedis, atau perusahaan teknologi yang memfasilitasi transaksi layanan kesehatan digital. Korporasi dapat dianggap bersalah apabila kebocoran data disebabkan oleh kebijakan manajemen yang buruk, kelalaian dalam menyediakan sistem keamanan digital, tidak adanya pelatihan keamanan data bagi karyawan, atau penggunaan perangkat lunak yang tidak memenuhi standar keamanan.

Pembagian tanggung jawab antara individu dan korporasi seringkali menjadi masalah kompleks. Misalnya, jika tenaga kesehatan menggunakan aplikasi telemedis resmi tetapi sistem aplikasinya mengalami kebocoran, maka korporasi penyedia sistem dapat dimintai pertanggungjawaban. Sebaliknya, apabila tenaga kesehatan menyalahgunakan akses pribadi, maka pertanggungjawaban sepenuhnya dapat jatuh pada individu yang bersangkutan.

Oleh karena itu, evaluasi pertanggungjawaban pidana dalam telemedis harus dilakukan secara komprehensif, mencermati hubungan antara teknologi, struktur organisasi, serta tingkat kewenangan tenaga kesehatan dalam mengelola data pasien.

Tantangan Penegakan Hukum dalam Pelanggaran Data Telemedis

Penegakan hukum terhadap pelanggaran data pasien dalam telemedis menghadapi beragam tantangan yang bersifat struktural, teknis, maupun regulatif. Tantangan pertama adalah minimnya literasi digital tenaga kesehatan. Banyak tenaga medis yang ahli dalam bidang klinis namun tidak familiar dengan standar keamanan siber, sehingga menjadi target empuk bagi rekayasa sosial dan kebocoran yang tidak disengaja. Tantangan kedua adalah keterbatasan kemampuan forensik digital di Indonesia. Kasus cybercrime, khususnya yang melibatkan sistem kesehatan digital, memerlukan teknik investigasi khusus seperti digital footprint tracking, malware analysis, atau server forensics. Sayangnya, banyak institusi penegak hukum belum memiliki sumber daya memadai untuk melakukan investigasi secara cepat dan komprehensif.

Tantangan berikutnya adalah ketidakjelasan regulasi turunan dari UU Kesehatan dan UU PDP. Sampai saat ini belum ada standar baku nasional mengenai keamanan data telemedis, sehingga setiap fasilitas kesehatan memiliki aturan dan kemampuan berbeda-beda. Akibatnya, ada kesenjangan keamanan yang cukup lebar antara rumah sakit besar dan fasilitas kesehatan kecil, terutama di daerah rural.

Selain itu, penegakan hukum juga terhambat oleh keterbatasan SOP keamanan, kurangnya anggaran digitalisasi, dan resistensi tenaga kesehatan terhadap perubahan teknologi. Banyak rumah sakit masih menggunakan sistem manual atau semi-digital sehingga integrasi ke telemedis menimbulkan risiko tambahan. Di sisi lain, ancaman serangan siber semakin canggih dan terorganisir, termasuk serangan dari luar negeri. Secara keseluruhan, penegakan hukum dalam telemedis menuntut modernisasi sistem keamanan, peningkatan kapasitas aparat, serta harmonisasi regulasi lintas sektor.

Usulan Penguatan Regulasi dan Sistem Pengawasan

Perlindungan data pasien berbasis telemedis membutuhkan reformasi hukum dan kebijakan yang bersifat komprehensif serta adaptif dengan perkembangan teknologi. Pertama, dibutuhkan standar keamanan nasional untuk telemedis, mencakup enkripsi end-to-end, sertifikasi server kesehatan, autentikasi multi-faktor, penggunaan firewall berlapis, dan audit sistem secara periodik. Standar keamanan ini harus menjadi kewajiban legal bagi seluruh penyedia layanan kesehatan digital.

Kedua, pemerintah perlu menerbitkan peraturan turunan yang memberikan kepastian pembagian tanggung jawab antara tenaga kesehatan, fasilitas pelayanan kesehatan, dan platform telemedis. Dengan adanya pembagian peran yang jelas, mekanisme pertanggungjawaban pidana dapat ditegakkan tanpa ambiguitas. Ketiga, tenaga kesehatan wajib mengikuti pelatihan keamanan digital yang diselenggarakan secara berkala. Pelatihan ini bertujuan meningkatkan kemampuan tenaga kesehatan dalam mengenali ancaman siber, mengelola data secara aman, dan mematuhi protokol hukum terkait perlindungan data.

Keempat, pembentukan Satuan Siber Kesehatan Nasional menjadi kebutuhan mendesak. Satuan ini akan bekerja sama dengan BSSN dan Kementerian Kesehatan untuk melakukan pengawasan, investigasi, dan mitigasi pada kasus kebocoran data pasien. Kelima, kerja sama internasional harus diperluas mengingat banyak serangan siber berasal dari jaringan global. Indonesia perlu berkolaborasi dengan WHO, Interpol, dan lembaga internasional lainnya untuk mengembangkan sistem respons digital terhadap ancaman internasional. Dengan berbagai langkah ini, keamanan data pasien dalam telemedis dapat ditingkatkan dan implementasi hukum pidana kesehatan akan menjadi lebih efektif serta berkeadilan.

KESIMPULAN

Perkembangan telemedis dalam sistem pelayanan kesehatan Indonesia membawa manfaat besar berupa peningkatan akses, efisiensi, dan jangkauan layanan kesehatan, khususnya bagi masyarakat di wilayah terpencil. Namun, digitalisasi layanan kesehatan juga menimbulkan risiko serius terhadap keamanan dan kerahasiaan data pasien yang tergolong data pribadi sensitif. Berdasarkan ketentuan UU Kesehatan No. 17 Tahun 2023 dan UU PDP No. 27 Tahun 2022, tenaga kesehatan dan penyelenggara layanan berkewajiban menjaga integritas, kerahasiaan, dan keamanan data pasien sehingga setiap pelanggaran dapat menimbulkan konsekuensi pidana.

Hasil penelitian menunjukkan bahwa pertanggungjawaban pidana tenaga kesehatan dalam kasus kebocoran data bergantung pada ada atau tidaknya unsur kesengajaan, kelalaian berat, atau tindakan yang

bertentangan dengan standar profesi. Namun, ekosistem telemedis yang kompleks menjadikan tanggung jawab tidak hanya melekat pada tenaga kesehatan, melainkan juga pada fasilitas kesehatan, penyedia aplikasi, pengelola server, dan pihak ketiga lainnya. Kebocoran data dapat terjadi melalui kelalaian individu, kelemahan sistem, serangan siber, maupun penyalahgunaan internal, sehingga penanganannya membutuhkan pendekatan yang komprehensif.

Penelitian ini juga menemukan bahwa penegakan hukum menghadapi sejumlah kendala, termasuk lemahnya literasi digital tenaga kesehatan, kurangnya kemampuan forensik digital, belum adanya standar keamanan nasional untuk telemedis, serta kesenjangan kualitas sistem keamanan antar fasilitas kesehatan. Untuk itu, diperlukan reformasi regulasi yang lebih tegas dan adaptif, termasuk penetapan standar keamanan digital nasional, pengaturan pembagian tanggung jawab pidana secara lebih rinci, peningkatan pelatihan keamanan digital bagi tenaga kesehatan, serta pembentukan mekanisme pengawasan dan respons siber yang terintegrasi.

Dengan pembaruan regulatif dan penguatan sistem keamanan digital, perlindungan data pasien dalam layanan telemedis dapat diwujudkan secara lebih efektif, sehingga kepercayaan publik dan integritas pelayanan kesehatan digital dapat terjamin.

DAFTAR PUSTAKA

Karim, M. (2023). *Hukum Pidana Indonesia*. Jakarta: Prenada Media Group.

Marzuki, P. M. (2016). *Penelitian Hukum* (Edisi Revisi). Jakarta: Prenada Media / Kencana.

Triwibowo, C. (2020). *Etika dan Hukum Kesehatan*. Yogyakarta: Nuha Medika.

World Health Organization. (2010). *Telemedicine: Opportunities and Developments in Member States — Report on the Second Global Survey on eHealth* (Global Observatory for eHealth Series, Vol. 2). Geneva: WHO.

Badan Siber dan Sandi Negara (BSSN). (2023). Laporan Ancaman Siber Sektor Kesehatan.

Kemenkes RI. (2024). Roadmap Transformasi Digital Kesehatan Nasional.

Interpol. (2022). Cybercrime and Critical Health Infrastructure Report.

Arfah, N. A., & Puspitosari, H. (2023). *Perlindungan Hukum Terhadap Data Pasien Telemedicine dalam Penerimaan Pelayanan Medis Berbasis Online.* Jurnal Hukum Fusion, 3(2), 45–56.

Lestari, R. D. (2022). *Perlindungan Hukum bagi Pasien dalam Telemedicine di Indonesia.* Jurnal Cendekia Ilmu Hukum, 6(1), 101–115.

Mutiah, F., Sibuea, H., & Candra, M. (2023). *Telemedicine Regulation in Indonesia: Legal Frameworks, Challenges, and Future Directions.* Jurnal Manajemen Informasi, 7(3), 221–234.

Jannah, M., Amboro, F. Y. P., & Shahrullah, R. (2024). *Personal Data Protection in Telemedicine: Comparison of Indonesian and EU Law.* Jurnal Legalitas dan Perlindungan Teknologi, 5(1), 12–28.

Ramadhani, S. (2021). *Tinjauan Yuridis Kebocoran Data Pribadi dalam Pelayanan Kesehatan Digital.* Jurnal Hukum dan Teknologi, 9(2), 88–102.

Putri, P. A., & Salsabila, N. (2023). *Analisis Yuridis Keamanan Data Pasien dalam Telemedicine Berdasarkan UU PDP.* Jurnal Hukum & Teknologi Indonesia, 5(2), 99–114.

Wahyuningtyas, N. (2021). *Pertanggungjawaban Pidana dalam Kebocoran Data Pribadi di Era Digital.* Jurnal Hukum Pidana dan Teknologi, 3(1), 55–70.

Malik, M., & Tuma, P. (2022). *Legal Liability in Telemedicine Platforms: A Comparative Review*. Journal of Health Law & Policy, 45(3), 311–329

Gostin, L. O., Halabi, S. F., & Wilson, K. (2022). *Health Data Protection and the Law: Governing Telemedicine in the Digital Era.* Journal of Law, Medicine & Ethics, 50(1), 7–20.

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

Indonesia. (2023). Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan.

Kitab Undang-Undang Hukum Pidana (KUHP).