

**STUDI KASUS PERLINDUNGAN DATA PASIEN DAN
TELEMEDISIN : TINJAUAN REGULASI DAN PRAKTIK DI
INDONESIA**

Ruben A. Riupassa¹, Rospita Adelina Siregar², Mompang L. Panggabean³
ruben.riupassa@gmail.com¹, rospita.siregar@uki.ac.id², mompang.panggabean@uki.ac.id³
Universitas Kristen Indonesia

Abstrak: Perkembangan teknologi digital telah membawa transformasi signifikan dalam layanan kesehatan, salah satunya melalui telemedisin. Di Indonesia, penggunaan telemedisin meningkat pesat terutama sejak pandemi COVID-19. Namun, perkembangan ini juga menimbulkan tantangan baru dalam hal perlindungan data pribadi pasien. Studi ini bertujuan untuk menganalisis praktik perlindungan data pada platform telemedisin serta mengevaluasi kepatuhannya terhadap regulasi yang berlaku, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan regulasi sektor kesehatan. Metode yang digunakan adalah studi kualitatif deskriptif dengan pendekatan studi kasus terhadap salah satu penyedia layanan telemedisin di Indonesia. Hasil penelitian menunjukkan bahwa meskipun terdapat upaya pengamanan data, masih ditemukan kelemahan pada aspek transparansi, persetujuan pengguna, dan pengelolaan data. Studi ini merekomendasikan penguatan kebijakan perlindungan data serta peningkatan literasi digital di kalangan pasien dan tenaga medis.

Kata Kunci: Telemedisin, Perlindungan Data, Privasi Pasien, Regulasi, Indonesia.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) telah mengubah banyak aspek kehidupan manusia, termasuk di bidang pelayanan kesehatan. Digitalisasi dalam sektor kesehatan membawa perubahan paradigma dalam penyampaian layanan kepada masyarakat. Salah satu bentuk inovasi yang paling menonjol adalah hadirnya layanan telemedisin, yaitu praktik pelayanan kesehatan yang dilakukan dari jarak jauh menggunakan perangkat digital.

Di Indonesia, perkembangan layanan telemedisin mengalami akselerasi pesat terutama sejak pandemi COVID-19 melanda pada awal tahun 2020. Pembatasan aktivitas fisik dan kebutuhan mendesak akan layanan kesehatan mendorong masyarakat untuk beralih ke konsultasi jarak jauh. Platform seperti Halodoc, Alodokter, SehatQ dan beberapa platform digital lainnya menjadi solusi cepat dalam memenuhi kebutuhan tersebut.

Telemedisin memberikan berbagai manfaat, seperti efisiensi waktu, pengurangan beban fasilitas kesehatan, serta aksesibilitas layanan di wilayah terpencil. Namun, kemudahan ini juga membawa risiko, terutama terkait dengan keamanan dan perlindungan data pribadi pasien. Informasi medis merupakan data yang sangat sensitif, dan kebocoran atau penyalahgunaannya dapat menimbulkan dampak serius bagi individu maupun institusi penyedia layanan.

Di tengah pesatnya perkembangan telemedisin, muncul kekhawatiran publik mengenai sejauh mana data pribadi pasien terlindungi dalam ekosistem digital tersebut. Banyak kasus kebocoran data yang mulai terungkap, yang menunjukkan lemahnya sistem keamanan dan tata kelola data oleh penyelenggara layanan. Salah satu insiden yang sempat menjadi sorotan adalah dugaan kebocoran data pengguna platform Halodoc pada tahun 2020.

Regulasi terkait perlindungan data pribadi di Indonesia mengalami perkembangan signifikan dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). UU ini memberikan kerangka hukum yang lebih kuat bagi perlindungan hak-hak subjek data, termasuk pasien dalam layanan kesehatan digital. Di samping itu, sektor kesehatan juga memiliki regulasi sektoral seperti Peraturan Menteri Kesehatan No. 20 Tahun 2019 tentang Penyelenggaraan Pelayanan Telemedisin.

Namun, adanya regulasi belum tentu menjamin efektivitas pelaksanaannya di lapangan. Masih ditemukan celah dalam implementasi prinsip-prinsip perlindungan data, seperti transparansi, persetujuan yang sah, batasan pemrosesan, dan mekanisme pelaporan insiden. Hal ini menimbulkan pertanyaan mengenai kesiapan para pelaku industri kesehatan digital dalam memenuhi standar perlindungan data.

Masalah lainnya adalah rendahnya literasi digital di kalangan pengguna layanan, baik pasien maupun tenaga medis. Banyak pasien yang tidak memahami bagaimana data mereka diproses dan disimpan oleh platform digital. Akibatnya, mereka kurang menyadari hak-hak mereka sebagai subjek data, seperti hak atas akses, koreksi, penghapusan data, dan penarikan persetujuan.

Selain itu, Indonesia menghadapi tantangan dalam hal infrastruktur keamanan siber yang belum merata. Tidak semua penyedia layanan memiliki kemampuan teknis dan sumber daya untuk menerapkan sistem keamanan informasi yang andal. Hal ini diperparah oleh kurangnya audit dan pengawasan dari lembaga regulator terhadap penyelenggara layanan telemedisin.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengkaji lebih dalam praktik perlindungan data pasien pada platform telemedisin di Indonesia, dengan fokus pada studi kasus Halodoc. Penelitian ini akan mengevaluasi kepatuhan platform terhadap regulasi yang berlaku serta menganalisis kelemahan dan tantangan yang dihadapi dalam pelaksanaannya.

Dengan pendekatan kualitatif dan studi kasus, penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan kebijakan perlindungan data di sektor kesehatan digital. Temuan dari studi ini juga diharapkan dapat meningkatkan kesadaran semua pihak terkait pentingnya privasi dan keamanan data pasien dalam era layanan kesehatan berbasis teknologi.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus. Objek studi adalah platform telemedisin Halodoc yang aktif di Indonesia. Teknik pengumpulan data dilakukan melalui studi dokumen, observasi terhadap kebijakan privasi dan alur penggunaan layanan, serta analisis pemberitaan media massa. Analisis data dilakukan dengan pendekatan deskriptif dan interpretatif terhadap regulasi.

PEMBAHASAN

Profil Platform Telemedisin yang Diteliti

Halodoc merupakan salah satu platform layanan kesehatan digital terbesar di Indonesia yang menyediakan layanan konsultasi dokter, pembelian obat, dan pemeriksaan laboratorium. Platform ini mengharuskan pengguna membuat akun dan mengunggah data pribadi serta riwayat kesehatan.

Berdasarkan laporan Katadata kuartal II 2020, Halodoc telah digunakan lebih dari 20 juta pengguna aktif bulanan; jumlah ini meningkat sepuluh kali lipat di masa pandemi COVID-19. Laporan Bisnis.com per 16 Februari 2025 menyatakan Halodoc kini memiliki 20 juta pengguna aktif bulanan, termasuk layanan kesehatan mental. Sedangkan menurut IDN Times dan Republika, Alodokter memiliki lebih dari 30 juta pengguna aktif per bulan serta lebih dari 30 ribu dokter yang terdaftar. Selain itu, Katadata menyebut platform ini memiliki sedikitnya 30 juta pengguna aktif serta lebih dari 43.000 dokter aktif.

Kedua platform tersebut mendominasi pasar telemedicine di Indonesia, dengan Alodokter unggul dari sisi jumlah pengguna aktif, sedangkan Halodoc lebih menonjol dari sisi adopsi cepat selama pandemi dan layanan kesehatan mental.

Berdasarkan rilis resmi dari AWS (Mei 2023), Halodoc memiliki lebih dari 20.000 dokter berlisensi yang bekerja melalui platform mereka. Data dari Digital News Asia (2018) menyebutkan Halodoc menggaet 22.000 dokter berlisensi, dengan 150–200 dokter aktif per hari. Mime Asia (2018) melaporkan kolaborasi Halodoc dengan 20.000 dokter, kini juga melayani lebih dari 20 juta pengguna per bulan. Jadi, estimasi terkini menunjukkan Halodoc memiliki sekitar 20.000–22.000 dokter di platform mereka. Sedangkan menurut laporan DailySocial (Nov 2023) menyebutkan ada 1.000 dokter umum dan 500 dokter spesialis, jadi total ± 1.500 dokter yang terdaftar pada aplikasi Alodokter. Selain itu, platform “Alomedika” yang berafiliasi dengan Alodokter mencatat partisipasi lima dari 95.000 dokter di seluruh Indonesia, tetapi ini lebih ke komunitas profesional, bukan dokter yang aktif melayani pasien lewat telemedisin. Jadi, Alodokter memperkirakan jumlah dokter yang aktif memberikan layanan telemedisin adalah sekitar 1.500 orang.

Halodoc memiliki jangkauan tenaga medis yang jauh lebih besar, dari ribuan generalis hingga spesialis, sementara Alodokter meskipun lebih kecil jumlah dokternya, menawarkan kombinasi dokter umum dan spesialis dalam jumlah signifikan.

Kasus Kebocoran Data Halodoc (2020)

Pada tahun 2020, sempat muncul laporan bahwa data pengguna Halodoc, termasuk foto hasil pemeriksaan laboratorium, dapat diakses publik melalui tautan tertentu. Hal ini dilaporkan oleh pihak eksternal melalui platform Twitter dan sempat ramai diberitakan oleh media nasional. Meskipun Halodoc segera memperbaiki celah keamanan tersebut, insiden ini menimbulkan pertanyaan serius mengenai sistem perlindungan data dan transparansi penanganan pelanggaran.

Data yang diduga bocor meliputi: nama lengkap pasien, tanggal pemeriksaan, jenis pemeriksaan laboratorium, hasil tes laboratorium (misalnya tes darah, tes COVID-19), foto digital hasil pemeriksaan dan lokasi laboratorium/klinik. Jenis data ini tergolong sebagai data pribadi sensitif menurut Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), karena berhubungan langsung dengan kondisi kesehatan individu.

Kebocoran ini terjadi bukan akibat peretasan, tetapi karena pengelolaan akses data yang tidak aman. Tautan langsung (direct links) hasil lab tidak dienkripsi atau tidak memiliki batas akses. Tidak ada pembatasan sesi login atau token akses yang membatasi waktu dan identitas pengguna. Tidak diterapkan akses berbasis izin (access control) yang cukup rinci dan detail. Hal ini menunjukkan kelemahan dalam sistem manajemen data, bukan semata-mata kegagalan infrastruktur IT.

Halodoc mengklaim telah menutup celah begitu laporan muncul. Tidak ada publikasi resmi terkait jumlah pengguna yang terdampak, durasi insiden, atau prosedur mitigasi. Tidak jelas apakah dilakukan pemberitahuan resmi kepada pengguna yang datanya bocor. Ketidadaan transparansi ini bertentangan dengan prinsip-prinsip notifikasi pelanggaran data sebagaimana diatur dalam praktik internasional seperti GDPR (General Data Protection Regulation).

Kebocoran ini melanggar prinsip kerahasiaan pasien (confidentiality) yang menjadi dasar etika profesi medis. Hal ini dapat berdampak kepada penurunan kepercayaan masyarakat terhadap layanan telemedisin. Pada saat insiden terjadi, UU PDP belum diberlakukan. Namun, kewajiban perlindungan data sebenarnya telah tercantum dalam:

- UU ITE (Informasi dan Transaksi Elektronik)
- Permenkes No. 269/Menkes/Per/III/2008 tentang Rekam Medis
- Permenkes No. 20 Tahun 2019 tentang Telemedisin antar Fasilitas Pelayanan Kesehatan

Jika insiden terjadi pasca 2022, Halodoc bisa terkena sanksi administratif hingga pidana sesuai Pasal 57 dan Pasal 67 UU PDP. Kebocoran data Halodoc tahun 2020 bukan hanya masalah teknis, tetapi mencerminkan lemahnya tata kelola data dalam ekosistem digital kesehatan. Meskipun layanan telemedisin memberi banyak manfaat, risiko keamanan informasi tidak boleh diabaikan. Dibutuhkan regulasi yang tegas, audit berkala, dan edukasi menyeluruh untuk memastikan data pasien tetap terlindungi.

Analisis Perlindungan Data

Ditemukan bahwa Halodoc telah memiliki kebijakan privasi yang cukup rinci, namun pengguna sering kali tidak membaca atau memahami isi kebijakan tersebut. Proses persetujuan penggunaan data dilakukan secara implisit melalui klik “setuju”, tanpa adanya edukasi lanjutan mengenai hak pengguna. Selain itu, belum ada mekanisme publik untuk melaporkan pelanggaran data secara transparan.

Sebagian besar platform telemedisin di Indonesia, termasuk Halodoc dan Alodokter, telah memiliki dokumen kebijakan privasi yang secara garis besar mencantumkan jenis data yang dikumpulkan (data identitas, rekam medis, lokasi, metode pembayaran); tujuan pengumpulan data; prosedur penyimpanan dan perlindungan data; hak-hak pengguna (akses, perbaikan, penghapusan); dan persetujuan terkait kemungkinan pihak ketiga yang dapat menerima data (misalnya, mitra farmasi atau laboratorium). Kebijakan ini seringkali ditulis dalam bahasa hukum yang sulit dipahami pengguna awam, dan persetujuan biasanya bersifat “terpaksa” (forced consent) melalui tombol “Setuju” saat awal pendaftaran tanpa pilihan granular (opt-in/out) atas jenis data yang dibagikan.

UU No. 27 Tahun 2022 (UU PDP) mewajibkan bahwa pengumpulan data pribadi sensitif hanya boleh dilakukan atas dasar persetujuan eksplisit (consent) dan tertulis dari subjek data. Fakta yang kerap terjadi di lapangan platform umumnya hanya meminta persetujuan umum satu kali didepan saat pendaftaran. Tidak terdapat pemisahan antara persetujuan untuk data identitas dan data medis (lack of informed consent). Tidak ada log historis yang bisa diakses pengguna terkait kapan dan untuk tujuan apa datanya pernah diakses atau diproses.

Secara umum sebenarnya setiap platform telah memiliki prosedur keamanan data. Platform yang diteliti menyatakan telah menerapkan beberapa teknologi keamanan berupa enkripsi data dalam transmisi dan penyimpanan (e.g., SSL/TLS); autentikasi dua faktor (2FA) untuk login pengguna dan tenaga medis; dan tersedianya log akses sistem untuk memantau aktivitas dalam sistem. Meskipun teknologi keamanan digunakan, penerapannya belum konsisten di seluruh titik akses sistem. Tidak

semua komunikasi internal (antara admin, dokter, atau mitra pihak ketiga) menggunakan saluran terenkripsi penuh. Belum ada jaminan atau pernyataan tentang adanya audit eksternal berkala atau penerapan standar internasional seperti ISO 27001 atau HIPAA.

Salah satu prinsip perlindungan data adalah data minimization dan storage limitation – artinya data yang dikumpulkan harus terbatas pada yang diperlukan, dan disimpan hanya selama dibutuhkan. Platform menyimpan data pengguna secara tidak terbatas waktu (no retention policy jelas). Tidak terdapat fitur bagi pengguna untuk menghapus akun atau menghapus permanen data medis yang telah dikumpulkan. Permintaan penghapusan data biasanya harus dilakukan secara manual via email dan tidak ada jaminan bahwa penghapusan dilakukan secara menyeluruh dan berhasil.

Terlihat pengungkapan dan transfer data ke pihak ketiga biasanya dalam kebijakan privasi menyebutkan bahwa data dapat dibagikan ke pihak ketiga seperti mitra laboratorium, farmasi mitra pengiriman obat, asuransi kesehatan; dan/atau penyedia cloud hosting. Tidak ada transparansi tentang siapa pihak ketiga tersebut dan bagaimana mereka mengelola data. Tidak dijelaskan apakah pihak ketiga telah menandatangani perjanjian perlindungan data (data processing agreement) ataupun pihak ketiga tersebut telah memiliki kebijakan pengamanan data yang setara dengan pihak platform. Disamping itu, potensi transfer data lintas negara (cross-border data transfer) tidak dijelaskan, padahal ini penting jika server berada di luar Indonesia.

Menurut Pasal 46–47 UU PDP, pengendali data wajib memberitahu pengguna dalam waktu 3x24 jam jika terjadi pelanggaran data (data breach). Kerap kali ditemukan bahwa tidak ada sistem pemberitahuan otomatis kepada pengguna jika terjadi kebocoran data. Dalam kasus kebocoran Halodoc 2020, tidak semua pengguna mengetahui bahwa data mereka mungkin bocor. Hal ini melanggar prinsip akuntabilitas dan responsibilitas dalam UU PDP.

UU PDP memberikan hak kepada subjek data untuk mengetahui pemrosesan data, menarik persetujuan, mengakses, memperbaiki, dan menghapus data serta mengajukan keberatan atas keputusan otomatis. Faktanya fitur ini belum sepenuhnya tersedia dalam aplikasi. Tidak ada sistem “data access request” yang mudah diakses pengguna. Pengguna harus mengirim email atau melakukan kontak manual untuk menggunakan hak-hak ini, dan tidak dijamin akan ditanggapi dengan cepat.

UU PDP baru berlaku penuh mulai 2024, namun sebagai penyelenggara sistem elektronik (PSE), platform telemedisin sudah semestinya siap dengan beberapa ketentuan minimum yang harus dipenuhi yaitu :

- Pengangkatan Petugas Perlindungan Data (Data Protection Officer / DPO)
- Mekanisme pencatatan dan pelaporan pelanggaran data
- Standar keamanan yang sesuai dengan regulasi

Belum semua platform secara terbuka mengumumkan penunjukan DPO. Mekanisme pelaporan pelanggaran tidak jelas dan tidak tersedia dalam aplikasi.

Evaluasi Kepatuhan Regulatif

Platform telah menerapkan langkah teknis seperti enkripsi dan autentikasi dua faktor, tetapi dalam praktiknya masih terdapat celah yang menunjukkan kurangnya audit berkala dan sistem pemberitahuan pelanggaran data kepada pengguna sebagaimana diatur dalam UU PDP. Ketidaksiapan dalam manajemen insiden data juga menunjukkan perlunya pengawasan eksternal yang lebih kuat.

Evaluasi kepatuhan terhadap regulasi dilakukan dengan membandingkan praktik yang diterapkan oleh penyedia layanan telemedisin (dalam studi ini, Halodoc sebagai contoh utama) terhadap ketentuan hukum dan prinsip perlindungan data yang berlaku di Indonesia. Fokus utama adalah pada kesesuaian dengan:

- Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)
- Peraturan Menteri Kesehatan Nomor 20 Tahun 2019 tentang Penyelenggaraan Pelayanan

Telemedisin

- Peraturan Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (sebagai pelengkap sebelum UU PDP berlaku penuh)

Kesesuaian dengan Prinsip UU PDP

UU PDP menetapkan prinsip-prinsip utama dalam pengelolaan data pribadi, antara lain:

Prinsip Utama	Fakta	Evaluasi
Keterbukaan dan Transparansi	Platform seperti Halodoc belum sepenuhnya memberikan transparansi terkait siapa yang mengakses data pasien dan untuk keperluan apa.	Belum patuh. Tidak tersedia notifikasi otomatis jika data diakses pihak ketiga.
Persetujuan yang Sah (Lawful Consent)	Persetujuan pengguna diberikan saat awal registrasi dengan format umum dan tanpa opsi yang detail.	Sebagian patuh. Persetujuan ada, namun tidak memenuhi kriteria eksplisit dan terpisah (informed and specific consent).
Tujuan Tertentu dan Terbatas (Purpose Limitation)	Data dikumpulkan untuk layanan medis, namun dapat juga digunakan untuk keperluan lain seperti promosi atau kemitraan farmasi.	Kurang patuh. Tidak selalu jelas tujuan sekunder pemrosesan data.
Keamanan dan Kerahasiaan Data	Sistem menggunakan enkripsi dan autentikasi ganda, namun belum terverifikasi standar keamanannya (seperti ISO 27001 atau audit independen).	Sebagian patuh. Ada praktik teknis yang memadai, namun tata kelola kelembagaan masih lemah.
Hak Subjek Data	Tidak ada fitur otomatis untuk akses atau penghapusan data oleh pengguna.	Tidak patuh. Hak subjek data belum difasilitasi secara sistemik
Pemberitahuan Pelanggaran Data	Pada insiden kebocoran tahun 2020, pengguna tidak diberi pemberitahuan resmi.	Tidak patuh. Melanggar Pasal 46 UU PDP tentang kewajiban notifikasi.

Kepatuhan terhadap Permenkes No. 20 Tahun 2019

Peraturan ini menekankan pada, kerahasiaan rekam medis pasien; penggunaan sistem yang aman dan tersertifikasi; penyimpanan data sesuai ketentuan Kementerian Kesehatan. Penyimpanan data dilakukan oleh penyedia platform tanpa pengawasan langsung dari Kementerian Kesehatan. Tidak tersedia informasi apakah sistem sudah mendapatkan standar keamanan TI atau audit kelaikan dari otoritas kesehatan. Pemantauan terhadap akses dokter terhadap data pasien belum tersedia secara terstruktur.

Evaluasi: Kepatuhan sebagian. Platform mengikuti standar internal, namun belum sepenuhnya sejalan dengan kontrol eksternal yang diatur dalam regulasi kesehatan.

Kepatuhan terhadap Peraturan Kominfo No. 20 Tahun 2016

Regulasi ini mewajibkan bahwa: 1).pengendali data untuk memiliki kebijakan perlindungan data; 2).Mekanisme untuk pengaduan dan penyelesaian sengketa; dan 3).Kewajiban melaporkan insiden kebocoran data

Evaluasi: Kebijakan perlindungan data tersedia namun tidak inklusif dan tidak dikomunikasikan dengan baik ke pengguna. Tidak ada kanal pengaduan yang tersedia secara

langsung dalam aplikasi. Tidak ada bukti bahwa pelaporan pelanggaran dilakukan ke Kominfo dalam insiden 2020. Dalam hal ini, platform berstatus tidak sepenuhnya patuh. Kebijakan ada tetapi implementasi lemahnya mengurangi efektivitas hukum.

Kelembagaan dan Tanggung Jawab

Menurut UU PDP, setiap pengendali data harus menunjuk Petugas Perlindungan Data (Data Protection Officer/DPO) dan memiliki sistem pengawasan internal. Tidak ditemukan informasi publik mengenai keberadaan DPO di platform yang diteliti. Pengawasan terhadap kebijakan internal tidak transparan. Dalam hal ini platform menjadi berstatus tidak patuh. Tidak sesuai dengan ketentuan tata kelola perlindungan data dalam Pasal 53–54 UU PDP.

Secara umum, platform telemedisin telah melakukan langkah-langkah awal dalam penerapan perlindungan data, namun masih terdapat banyak celah dalam kepatuhan terhadap UU PDP dan peraturan teknis lain. Tata kelola perlindungan data belum mapan, terutama dalam hal pemberitahuan, pengawasan akses, dan pelibatan pihak ketiga. Kepatuhan parsial ini berisiko terhadap sanksi hukum dan merusak kepercayaan publik dalam jangka panjang.

Implikasi Etis dan Sosial

Transformasi digital dalam bidang kesehatan melalui telemedisin membawa dampak besar, tidak hanya secara teknis, tetapi juga secara etis dan sosial. Penggunaan platform telemedisin seperti Halodoc dan Alodokter memperluas akses terhadap layanan medis, terutama bagi masyarakat yang tinggal jauh dari fasilitas kesehatan. Namun, kemudahan ini harus diseimbangkan dengan perlindungan terhadap hak-hak individu, khususnya hak atas privasi dan kendali atas data pribadi. Insiden kebocoran data menimbulkan kekhawatiran di masyarakat terhadap keamanan data kesehatan. Kurangnya literasi digital menyebabkan sebagian besar pasien tidak memahami risiko dan cara mengontrol informasi pribadi mereka. Hal ini berpotensi menurunkan kepercayaan publik terhadap layanan telemedisin.

Etika Privasi dan Kerahasiaan Medis

Secara etis, data medis memiliki karakteristik yang sangat sensitif karena berkaitan dengan kondisi tubuh, riwayat penyakit, kebiasaan hidup, dan bahkan informasi genetik seseorang. Dalam relasi antara pasien dan tenaga medis, terdapat prinsip dasar confidentiality (kerahasiaan) yang merupakan bagian integral dari kode etik profesi kedokteran.

Namun, dalam konteks layanan digital, prinsip ini menghadapi tantangan besar. Banyak platform tidak secara eksplisit menjelaskan bagaimana data pasien diproses, disimpan, dan digunakan, terutama ketika melibatkan pihak ketiga seperti perusahaan farmasi atau penyedia asuransi. Ketidakjelasan ini menimbulkan pertanyaan etis: apakah pasien benar-benar memberikan informed consent, atau hanya menekan tombol “Setuju” tanpa pemahaman memadai?

Ketimpangan Literasi Digital dan Hak Pasien

Secara sosial, tidak semua pengguna memiliki tingkat literasi digital yang cukup untuk memahami risiko dari pemanfaatan layanan telemedisin. Banyak pasien belum mengetahui bahwa mereka memiliki hak atas akses, perbaikan, hingga penghapusan data mereka. Ketimpangan ini terutama tampak di kalangan lansia, penduduk pedesaan, atau kelompok berpendidikan rendah.

Kondisi ini menciptakan asimetri informasi antara penyedia layanan dan pengguna. Pasien cenderung menyerahkan data secara pasif tanpa memahami implikasinya. Dalam banyak kasus, ketidaksadaran ini membuka peluang penyalahgunaan data, seperti untuk kepentingan pemasaran atau profiling komersial, yang secara etis tidak dapat dibenarkan jika tanpa persetujuan eksplisit.

Ancaman Terhadap Kepercayaan Publik

Isu kebocoran data, seperti yang terjadi pada Halodoc pada tahun 2020, menjadi contoh nyata bagaimana kurangnya perlindungan data dapat menggerus kepercayaan publik terhadap layanan kesehatan digital. Dalam jangka panjang, ketidakpercayaan ini dapat menghambat adopsi teknologi yang sebenarnya sangat potensial untuk meningkatkan efisiensi layanan kesehatan.

Kepercayaan adalah fondasi dalam hubungan antara pasien dan penyedia layanan. Ketika privasi dilanggar, kepercayaan tersebut runtuh. Hal ini bukan hanya berdampak pada satu platform, tetapi dapat meluas menjadi keraguan publik terhadap seluruh ekosistem layanan kesehatan berbasis teknologi.

Keadilan Sosial dan Aksesibilitas

Selain privasi, telemedisin juga menimbulkan pertanyaan mengenai keadilan sosial. Meskipun secara teori telemedisin dapat memperluas akses ke daerah terpencil, kenyataannya masih terdapat kesenjangan akses terhadap perangkat, konektivitas internet, dan keterampilan digital. Dengan kata lain, digitalisasi belum tentu inklusif.

Kebijakan kesehatan berbasis teknologi harus mempertimbangkan kelompok rentan yang mungkin tidak terjangkau oleh infrastruktur digital. Jika tidak, layanan ini justru memperlebar kesenjangan kesehatan antara kelompok masyarakat perkotaan dan pedesaan.

Etika Komersialisasi Data Kesehatan

Aspek lain yang perlu diperhatikan adalah tren komersialisasi data kesehatan. Beberapa platform menjalin kerja sama dengan pihak industri (seperti farmasi atau asuransi) untuk memanfaatkan data pengguna sebagai bahan analisis pasar. Jika dilakukan tanpa transparansi dan kontrol dari pengguna, praktik ini melanggar prinsip otonomi dan integritas individu.

Pasien berhak mengetahui apakah datanya digunakan untuk riset atau kepentingan komersial, serta memiliki hak untuk menolak tanpa konsekuensi terhadap akses layanan. Etika digital menuntut adanya batasan jelas antara layanan publik dan kepentingan bisnis.

KESIMPULAN

Telemedisin memiliki potensi besar dalam meningkatkan akses layanan kesehatan. Namun, perlindungan data pasien harus menjadi prioritas utama. Studi ini menyimpulkan bahwa implementasi perlindungan data pada layanan telemedisin di Indonesia, khususnya dalam kasus Halodoc, masih memerlukan perbaikan signifikan, terutama pada aspek transparansi, respons insiden, dan edukasi pengguna.

Implikasi etis dan sosial dari layanan telemedisin bersifat kompleks dan multidimensi. Di satu sisi, teknologi ini menjanjikan pemerataan akses kesehatan; di sisi lain, ia membuka ruang bagi pelanggaran privasi dan ketimpangan digital. Oleh karena itu, perlu ada pendekatan yang holistik, tidak hanya dari sisi teknis dan regulatif, tetapi juga dari dimensi etika, kesetaraan sosial, dan kesadaran masyarakat. Upaya peningkatan perlindungan data harus dibarengi dengan edukasi publik dan regulasi yang mampu menjamin bahwa kemajuan teknologi tidak mengorbankan hak dasar pasien sebagai individu yang bermartabat.

Berangkat dari kesimpulan ini maka berikut adalah beberapa rekomendasi yang coba ditawarkan :

1. Penegakan hukum yang lebih tegas terhadap pelanggaran data.
2. Edukasi masyarakat tentang hak-hak data pribadi.
3. Standarisasi kebijakan privasi oleh regulator.
4. Audit berkala terhadap platform layanan kesehatan digital.
5. Penerapan sistem notifikasi otomatis kepada pengguna jika terjadi pelanggaran data..

DAFTAR PUSTAKA

- Alodokter. (2021). Kebijakan Privasi. Diakses dari <https://www.alodokter.com/kebijakan-privasi>
- Halodoc. (2021). Kebijakan Privasi dan Syarat Ketentuan Pengguna. Diakses dari <https://www.halodoc.com>
- Kementerian Kesehatan Republik Indonesia. (2019). Peraturan Menteri Kesehatan Nomor 20 Tahun 2019 tentang Penyelenggaraan Pelayanan Telemedisin Antar Fasilitas Pelayanan Kesehatan.
- Kominfo. (2020). Penjelasan Isu Kebocoran Data Pasien di Halodoc. Diakses dari <https://www.kominfo.go.id>
- Kusnadi, D. (2023). Perlindungan Data Pribadi dalam Platform Telemedisin. *Jurnal Hukum dan Kesehatan*,

- 5(1), 22–35. <https://doi.org/10.1234/jhk.v5i1.123>
- Nugroho, Y., & Rachmawati, I. (2021). Tantangan Perlindungan Data Pasien pada Era Telemedicine. *Jurnal Informatika Kesehatan Indonesia*, 3(2), 45–56.
- Pusat Data dan Informasi Kementerian Kesehatan RI. (2022). Statistik Layanan Kesehatan Digital Indonesia 2022.
- Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 206.
- Warren, M., & Hutchinson, W. (2003). Cybersecurity and Healthcare: Avoiding Risk. *Computer Law & Security Report*, 19(6), 505–512. [https://doi.org/10.1016/S0267-3649\(03\)01101-2](https://doi.org/10.1016/S0267-3649(03)01101-2)
- World Health Organization (WHO). (2010). Telemedicine: Opportunities and Developments in Member States (Global Observatory for eHealth Series - Volume 2). Diakses dari https://www.who.int/goe/publications/goe_telemedicine_2010.pdf
- Yulianti, E. (2022). Dampak Sosial-Etika Telemedisin dan Perlindungan Privasi Pasien. *Jurnal Etika Teknologi dan Informasi*, 6(1), 15–28.