e-ISSN 2798-8260

Jurnal ISO: Jurnal Ilmu Sosial, Politik dan Humaniora Vol: 5, No 2, 2025, Page: 1-15

Penerapan Hukum Terhadap Pencurian Data *(Data Breach)* Pasien di Rumah Sakit

Nanik Widihastuti*, Rano Setia Budi, Ajat Sudrajat[3], Roy Wicaksono Michel Apon, Hernawati

Universitas Langlang Buana Bandung

Abstrak: Penelitian ini bertujuan untuk menganalisis penerapan hukum terhadap pencurian data (data breach) pasien di rumah sakit berdasarkan peraturan perundang-undangan di Indonesia, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, Undang-Undang Informasi dan Transaksi Elektronik, serta Peraturan Menteri Kesehatan tentang Rekam Medis dan Telemedicine. Metode penelitian yang digunakan adalah tinjauan literatur dengan pendekatan perundang-undangan dan konseptual, bersumber dari bahan hukum primer dan sekunder, guna mengkaji tanggung jawab hukum, bentuk sanksi, serta efektivitas regulasi dalam menangani kebocoran data pasien. Hasil penelitian menunjukkan bahwa data kesehatan termasuk kategori data pribadi yang bersifat spesifik sehingga memperoleh perlindungan hukum yang lebih ketat. Penerapan hukum terhadap pelaku pencurian data dapat berupa sanksi pidana, perdata, dan administratif, baik terhadap individu maupun korporasi sebagai pengendali data. Namun demikian, berbagai kasus kebocoran data yang terjadi menunjukkan bahwa implementasi regulasi belum optimal. Faktor penyebab meliputi lemahnya sistem keamanan siber, kelalaian sumber daya manusia, serta kurangnya pengawasan dan audit berkala. Oleh karena itu, diperlukan penguatan sistem keamanan digital, peningkatan literasi dan pelatihan keamanan data, pengawasan yang efektif, serta kolaborasi antara rumah sakit, pemerintah, dan masyarakat guna menjamin perlindungan data pasien secara komprehensif.

Kata Kunci: Penerapan Hukum, Pencurian Data, Pasien

DOI: https://doi.org/10.53697/iso.v5i2.3903
*Correspondence: Nanik Widihastuti
Email: nanikwidihastuti@gmail.com

Received: 30-10-2025
Accepted: 30-11-2025
Published: 30-12-2025

Abstract: *This study aims to analyze the legal enforcement against patient data theft (data breach) in hospitals under Indonesian laws and regulations, particularly Law Number 27 of 2022 on Personal Data Protection, Law Number 17 of 2023 on Health, the Law on Electronic Information and Transactions, and relevant Ministry of Health regulations concerning medical records and telemedicine. The research employs a literature review method using statutory and conceptual approaches, drawing on primary and secondary legal materials to examine legal responsibilities, types of sanctions, and the effectiveness of the regulatory framework in addressing patient data breaches. The findings indicate that health data are classified as specific personal data requiring stricter legal protection, and that legal enforcement against perpetrators may involve criminal, civil, and administrative sanctions imposed on both individuals and corporate entities acting as data controllers. However, recurring data breach incidents demonstrate that regulatory implementation remains suboptimal due to weak cybersecurity systems, human error, inadequate supervision, and the lack of regular security audits. Therefore, strengthening digital security systems, enhancing data protection training and literacy, improving oversight mechanisms, and fostering collaboration among hospitals, government institutions, and the public are essential to ensure comprehensive protection of patient data, maintain public trust, and uphold patients' rights in the era of digital health services.*

Keywords: *Application of Law, Data Theft, Patient*

Pendahuluan

Kebocoran data rumah sakit menjadi isu yang semakin menakutkan. Tidak hanya mengancam privasi pasien, namun juga menggerus kepercayaan masyarakat terhadap institusi layanan kesehatan. Dengan meningkatnya serangan siber yang menargetkan rumah sakit, sistem yang selama ini dianggap aman ternyata penuh celah. Ancaman ini tak mengenal waktu dan bisa menimpa rumah sakit dimana saja baik yang besar atau kecil.

Sesuai dengan UndangUndang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi terkait dengan adanya platform dan aplikasi kesehatan digital menjadi salah satu manifestasi digital yang menandai perubahan pola pelayanan kesehatan secara fundamental. Penerapan teknologi digital, seperti konsultasi daring (telemedicine), rekam medis elektronik (RME), serta aplikasi pemesanan obat secara daring, semakin berkembang di Indonesia. Inovasi-inovasi tersebut menambah mutu layanan Kesehatan bagi masyarakat, karena semakin efisiensi waktu dan biaya, khususnya bagi masyarakat yang tinggal di daerah dengan keterbatasan akses fasilitas Kesehatan (Annan, 2024).

Berdasarkan survei Kemenkes (2023) dan data BPS (2024) terkait penetrasi internet dan riset akademik menunjukkan tren peningkatan signifikan konseling online menjadi pilihan utama, dengan Perpres 82/2023 menjadi landasan transformasi digital nasional. Jurnal Syntax Literate (2024): Menunjukkan 46,5% pakai RS/Klinik telemedicine, 41,8% Alodokter, 35,7% konsultasi langsung, 20,3% KlikDokter.

Perlindungan data pribadi merupakan hal penting dalam kelangsungan rumah sakit, data pasien bersifat sangat sensitif dipakai untuk aplikasi digital, dan potensi kebocoran, penyalahgunaan, atau penggunaan ulang data tanpa persetujuan yang jelas berisiko melanggar hak privasi pasien. Regulasi perlindungan data nasional (termasuk aturan sektoral dan pedoman teknis kementerian) harus sejalan dengan praktik rekam medis elektronik sehingga prinsip-prinsip minimisasi data, enkripsi, anonimisasi/pseudonimisasi, serta persetujuan informasional. Dalam setiap insiden kebocoran data, yang sering dipersalahkan adalah manajemen rumah sakit atau penyedia sistem teknologi informasi.

Menurut Undang-Undang Perlindungan Data Pribadi (UU PDP), rumah sakit sebagai pengendali data wajib menjaga keamanan informasi pasien. Namun dalam praktiknya, tanggung jawab ini sering kali terabaikan atau dipindahkan ke vendor eksternal yang tidak selalu mematuhi standar keamanan tinggi. Dalam laporan yang dirilis oleh Badan Siber dan Sandi Negara (BSSN), disebutkan bahwa lebih dari 60% rumah sakit di Indonesia mengalami insiden kebocoran data dalam lima tahun terakhir. Ketika data bocor, dampaknya bukan hanya finansial, tetapi juga reputasional. Selain itu, pasien dapat menjadi korban penipuan, penyalahgunaan data medis, bahkan diskriminasi. Saat ini masih banyak rumah sakit yang menganggap keamanan data sebagai hal sekunder dibanding pengadaan alat medis.

Rumah sakit menjadi sasaran empuk bagi peretas karena kelemahan sistem, kelalaian manusia, dan kurangnya investasi keamanan. Banyak sistem informasi rumah sakit di Indonesia yang masih belum melakukan pembaruan keamanan secara berkala. Hal ini menjadi celah peretasan data. Selain itu, banyak staf rumah sakit yang belum terlatih menghadapi ancaman siber, sehingga sering kali menjadi target empuk teknik rekayasa sosial seperti phishing.

Laporan Trend Micro tahun 2024 menyebutkan bahwa sektor kesehatan berada di urutan ketiga sebagai target serangan siber terbanyak secara global, setelah keuangan dan pemerintahan. Di Asia Tenggara, serangan terhadap rumah sakit meningkat 80% dalam dua tahun terakhir. Tanpa adanya investasi signifikan terhadap jasa keamanan rumah sakit. Menurut riset dari Ponemon Institute, rata-rata biaya pelanggaran data di sektor kesehatan mencapai USD 10 juta per insiden—angka tertinggi dibanding sektor lain. Di Indonesia, meskipun nominal kerugian sering tak terpublikasi, dampaknya terlihat dari meningkatnya keluhan masyarakat terkait pencurian identitas dan pemalsuan dokumen medis.

Potensi manipulasi data medis, seperti data pasien yang diubah baik sengaja maupun tidak, bisa menyebabkan kesalahan diagnosis, pemberian obat yang salah, hingga kegagalan penanganan medis. Bagi pasien, ini adalah risiko nyawa. Oleh karena itu, rumah sakit harus mulai membangun sistem yang dapat menjamin integritas data, bukan sekadar menyimpannya.

Rekam medis elektronik mempermudah baik pasien maupun tenaga kesehatan dalam mengakses, mengelola, dan menyimpan data kesehatan secara aman dan terintegrasi (Yuliana, 2021). Namun, di balik berbagai manfaat tersebut, implementasi inovasi kesehatan digital juga memunculkan tantangan baru, khususnya terkait perlindungan hukum bagi pasien dan tenaga medis. Keamanan data, perlindungan privasi, dan kepastian hukum atas layanan kesehatan daring menjadi hal yang sangat penting dan perlu regulator dan pelaku layanan yang baik. Kebocoran data pribadi pasien berpotensi malpraktik maka harus ada pengaturan hukum yang komprehensif dan adaptif. Tenaga medis dan tenaga Kesehatan di rumah sakit membutuhkan kepastian hukum atas setiap tindakan yang dilakukan secara virtual, termasuk perlindungan dari tuntutan hukum apabila terjadi kendala teknis atau mispersepsi komunikasi dalam layanan digital (Pramukars, 2021).

Pengaturan mengenai inovasi kesehatan digital telah diatur dalam berbagai peraturan perundang-undangan seperti Undang-Undang Kesehatan, UndangUndang Praktik Kedokteran, Undang-Undang Perlindungan Data Pribadi, serta Peraturan Menteri Kesehatan yang lebih bersifat teknis, seperti mengenai penyelenggaraan rekam medis elektronik dan telemedicine. Berbagai regulasi tersebut mengamanatkan pentingnya perlindungan hukum yang seimbang antara kepentingan pasien dan tenaga medis sebagai pelaku utama dalam ekosistem layanan kesehatan digital (Dalimunthe, 2024). Masih banyak rumah sakit yang melakukan layanan kesehatan digital menghadapi kendala dalam memenuhi standar keamanan, infrastruktur teknologi, dan tata kelola perlindungan data sesuai ketentuan peraturan perundangan yang berlaku.

Perlindungan hukum, efektivitas kebijakan dan regulasi dalam mendukung pengembangan layanan digital kesehatan di Indonesia dipengaruhi oleh kesiapan infrastruktur, kapasitas sumber daya manusia, serta komitmen seluruh pemangku kepentingan. Kolaborasi lintas sektor diperlukan agar sistem kesehatan digital berjalan secara optimal dan mampu memberikan jaminan perlindungan bagi semua pihak yang terlibat. Perlindungan hukum bagi pasien sangat penting untuk menjamin hak-haknya, terutama terkait persetujuan tindakan medis, keamanan data pribadi, serta mekanisme pengaduan apabila terjadi pelanggaran dalam proses layanan digital. Di Indonesia, berbagai

bentuk aktivitas digital telah diatur melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, yang menjadi dasar hukum pengaturan penggunaan teknologi informasi, transaksi elektronik, perlindungan data pribadi, kejahatan siber, serta etika komunikasi digital. Berdasarkan kerangka regulasi tersebut, penelitian ini bertujuan untuk menganalisis penerapan dan efektivitas perlindungan hukum terhadap data pribadi pasien dalam layanan kesehatan digital serta mengkaji tanggung jawab hukum para pihak dalam mencegah dan menangani terjadinya pencurian atau kebocoran data pasien.

Metode Penelitian

Metode Penulisan yang digunakan tinjauan literatur dengan pendekatan perundang-undangan dan konseptual untuk menganalisis penerapan hukum terhadap pencurian Data (Data Breach) Pasien di Rumah Sakit bersumber dari bahan hukum primer berupa Undang-Undang Nomor 17 Tahun 2023 Tentang Kesehatan, Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya, serta peraturan perundang-undangan lainnya yang relevan. Bahan hukum sekunder terdiri atas literatur, jurnal ilmiah, artikel hukum.

Hasil dan Pembahasan

1. Konsep dan Karakteristik Pencurian Data Pasien

Definisi Data Breach	Jenis Data Dilindungi	Penyebab Umum	Risiko Utama

Deskripsi:

Pencurian data pasien merupakan tindakan akses, pengumpulan, atau penyebaran data medis sensitif tanpa izin. Faktor utama penyebab meliputi lemahnya keamanan siber, kurangnya pelatihan SDM, ancaman internal, dan audit sistem yang belum optimal. Insiden ini dapat menimbulkan kerugian finansial, gangguan layanan medis, serta pelanggaran terhadap regulasi perlindungan data seperti UU Perlindungan Data Pribadi.

2. Penyebab Pencurian Data

Keamanan Sistem	Kesalahan Manusia	Ancaman Internal	Kurangnya Audit

Deskripsi singkat:

Kerentanan sistem teknologi informasi rumah sakit, seperti tidak adanya enkripsi dan autentikasi ganda, menjadi celah utama serangan siber. Kurangnya pemahaman staf terhadap kebijakan keamanan data serta penyalahgunaan akses oleh oknum internal juga meningkatkan risiko kebocoran data pasien.

3. Dampak Kebocoran Data

Dampak bagi Pasien	Dampak bagi Rumah Sakit	Dampak Sistem Kesehatan	Dampak Ekonomi Global

Deskripsi singkat:
Pasien berpotensi mengalami pencurian identitas dan penipuan asuransi. Rumah sakit dapat mengalami kerugian finansial dan reputasi. Laporan IBM Cost of a Data Breach 2024 mencatat biaya kebocoran data global mencapai 4,88 juta dolar AS, sementara sektor kesehatan mencapai rata-rata 9,77 juta dolar AS akibat tingginya serangan ransomware.

4. Studi Kasus Kebocoran Data Kesehatan di Indonesia

a. Kasus Kebocoran Data COVID-19 Bali (2020)

Kronologi	Dugaan Penyebab	Dampak	Pelajaran yang Dipetik

Deskripsi singkat: Dugaan kebocoran 230.000 data pasien COVID-19 menimbulkan keresahan publik. Meskipun investigasi BSSN tidak menemukan bukti kebocoran resmi, kasus ini menunjukkan risiko kesalahan manusia, kelemahan sistem, serta kebocoran pihak ketiga. Peristiwa ini menekankan pentingnya audit keamanan, transparansi pemerintah, dan edukasi masyarakat terkait perlindungan data.

b. Kasus Kebocoran Data PeduliLindungi (2022)

Kronologi	Dugaan Penyebab	Dampak	Upaya Penanganan

Deskripsi singkat: Dugaan kebocoran ratusan juta data pengguna PeduliLindungi menunjukkan tingginya risiko kebocoran data pada sistem kesehatan digital. Kemungkinan penyebab meliputi replikasi data yang tidak aman, celah infrastruktur, serta serangan malware. Pemerintah melakukan investigasi, perbaikan sistem keamanan, dan pemberitahuan kepada pengguna sebagai langkah mitigasi.

5. Tantangan Implementasi Perlindungan Data Kesehatan

Infrastruktur	SDM	Pengawasan	Integrasi Sistem

Deskripsi singkat: Transformasi digital kesehatan di Indonesia masih menghadapi kendala kesiapan teknologi, literasi digital tenaga medis, serta belum optimalnya integrasi sistem layanan kesehatan. Banyak fasilitas kesehatan belum memenuhi standar keamanan data secara menyeluruh.

6. Perlindungan Hukum

UU PDP	UU Kesehatan	UU ITE	Permenkes Rekam Medis & Telemedicine

Deskripsi singkat:
Perlindungan hukum data pasien diatur melalui UU PDP, UU Kesehatan, UU ITE, serta Permenkes terkait rekam medis dan telemedicine. Regulasi tersebut menjamin hak pasien atas kerahasiaan data dan memberikan kepastian hukum bagi tenaga medis dalam layanan kesehatan digital.

7. Pertanggungjawaban Hukum

Individu Pelaku	Rumah Sakit (Pengendali Data)	Sanksi Pidana	Sanksi Administratif & Perdata

Deskripsi singkat:
Individu pelaku dapat dikenakan pidana penjara hingga enam tahun dan denda miliaran rupiah. Rumah sakit dapat dikenakan sanksi administratif, perdata, maupun pidana korporasi apabila terbukti lalai dalam melindungi data pasien.

8. Upaya Pencegahan dan Solusi

Penguatan Sistem Keamanan	Pelatihan SDM	Kepatuhan Regulasi	Kolaborasi Multi-Pihak

Deskripsi singkat:
Pencegahan dilakukan melalui enkripsi, autentikasi multi-faktor, audit keamanan berkala, pembatasan akses berbasis peran, serta pembentukan tim tanggap insiden siber. Kolaborasi antara pemerintah, institusi kesehatan, penyedia teknologi, dan masyarakat sangat diperlukan.

Pelajaran yang Dipetik
Kebocoran data Covid-19 di Bali menjadi pengingat penting tentang pentingnya menjaga keamanan data pribadi, terutama di tengah pandemi. Berikut beberapa pelajaran berharga dari peristiwa ini:

- Memperkuat Keamanan Data Pribadi: Data kesehatan harus dilindungi dengan protokol yang ketat, termasuk penggunaan teknologi enkripsi dan pembatasan akses, serta melatih karyawan tentang pentingnya keamanan data.
- Edukasi Masyarakat: Kampanye publik dan seminar diperlukan untuk meningkatkan kesadaran masyarakat tentang pelindungan data pribadi dan hak-hak mereka terkait hal ini.
- Penegakan Hukum yang Tegas: Pelaku kebocoran data harus ditindak dengan tegas untuk mencegah pelanggaran serupa di masa depan dan membangun kepercayaan masyarakat terhadap pemerintah.
- Transparansi dan Akuntabilitas: Pemerintah harus transparan tentang pengelolaan data pribadi dan melibatkan masyarakat dalam pengambilan keputusan terkait data mereka.

Sumber

- Bali Express. (2020, Juni 22). *Beredar di Medsos, Data Pasien Covid-19 Bali Diduga Dijual*. Diakses dari baliexpress.jawapos.com
- Bali Post. (2020, Juni 22). *Data Pasien Covid-19 di Bali Diduga, Memang Mau Diapain Datanya?* Diakses dari www.balipost.com
- Kompas.com. (2020, Juni 22). *Data Pasien Covid-19, Dirahasiakan Pemerintah, Diduga Dijual Hacker...*Diakses dari nasional.kompas.com

- Tribun-Bali. (2020, Juni 22). *Polda Bali Dalami Dugaan Kebocoran Data Covid-19 di Bali*. Diakses dari bali.tribunnews.com

1. Kebocoran Data PeduliLindungi (2022)

Deskripsi Insiden

Pada November 2022, Indonesia digemparkan dengan dugaan kebocoran data 472 juta pengguna aplikasi PeduliLindungi, yang merupakan platform resmi pemerintah Indonesia untuk melacak pergerakan dan status kesehatan masyarakat selama pandemi COVID-19. Data yang bocor termasuk informasi pribadi yang sangat sensitif, seperti nama lengkap, Nomor Induk Kependudukan (NIK), nomor telepon, alamat, riwayat vaksinasi, dan hasil tes COVID-19. Insiden ini mengejutkan publik dan menimbulkan kekhawatiran besar mengenai keamanan data pribadi di Indonesia, terutama terkait dengan aplikasi yang seharusnya digunakan untuk menjaga kesehatan masyarakat di tengah pandemi.

Kebocoran data ini pertama kali terungkap pada 15 November 2022, ketika tim *Cyber Threat Intelligence* Badan Siber dan Sandi Negara (BSSN) melaporkan temuan data yang dijual di forum Deep Web bernama breached.to. Peretas yang dikenal dengan nama Bjorka mengklaim memiliki 3,25 miliar data, sebesar 157 GB, yang mencakup data vaksinasi, riwayat check-in, dan data kontak tracing pengguna aplikasi PeduliLindungi. Bjorka memberikan 40 record sampel data secara gratis dan menawarkan seluruh kumpulan data tersebut seharga USD 100 ribu dalam bentuk bitcoin. Meskipun hanya 94 juta pengguna yang disebutkan dalam data tersebut, dugaan kebocoran ini tetap menjadi perhatian besar, mengingat jumlah data yang terungkap sangat signifikan.

Pakar keamanan siber, seperti Pratama Persadha, serta analisa dari Alfons Tanujaya, mengonfirmasi validitas data yang bocor, semakin menambah kekhawatiran masyarakat. Tanujaya bahkan mengkritik pihak yang mengelola aplikasi PeduliLindungi, menyatakan bahwa mereka gagal dalam menjaga keamanan data yang sangat besar ini. Menanggapi insiden tersebut, BSSN, Kementerian Kesehatan (Kemenkes), Kementerian Komunikasi dan Informatika (Kemenkominfo), dan PT Telkom segera berkoordinasi untuk menangani situasi. Mereka melakukan investigasi dan validasi data untuk memastikan kebenaran kebocoran tersebut, serta menyelidiki penyebab dan kerentanannya. Selama proses ini, berbagai langkah perbaikan sistem dan penyempurnaan protokol keamanan dilaksanakan untuk mencegah kebocoran serupa di masa depan.

Insiden ini menyoroti betapa pentingnya regulasi yang lebih ketat serta kesadaran yang lebih tinggi terkait pelindungan data pribadi di era digital. Pemerintah Indonesia mengambil langkah transparansi dengan memberi informasi terkini kepada publik mengenai perkembangan penanganan kebocoran data ini, serta memberi jaminan bahwa langkah-langkah preventif sedang diterapkan. Kejadian ini juga menekankan pentingnya kerjasama antara pemerintah, penyedia layanan teknologi, dan masyarakat dalam menjaga keamanan data. Selain memperkuat sistem keamanan, edukasi kepada pengguna mengenai cara melindungi data pribadi mereka menjadi hal yang sangat penting. Insiden ini seharusnya menjadi pelajaran berharga untuk semua pihak dalam memahami bahaya kebocoran data dan pentingnya menjaga kerahasiaan informasi pribadi.

Kronologi

- 13 November 2022 – *Kebocoran Data Klaim Bjorka*: Bjorka, seorang peretas, memposting sampel data di forum online breached.to dan mengklaim memiliki 3,25 miliar data pengguna PeduliLindungi. Data yang diposting mencakup informasi sensitif yang memicu kekhawatiran.
- 15 November 2022 – *Konfirmasi BSSN*: BSSN (Badan Siber dan Sandi Negara) mengonfirmasi adanya dugaan kebocoran data dari sistem PeduliLindungi, yang kemudian menarik perhatian publik dan media.
- 16 November 2022 – *Penegasan Kemenkes*: Kementerian Kesehatan (Kemenkes) menyatakan bahwa data yang bocor tidak berasal dari sistem PeduliLindungi. Pernyataan ini bertujuan untuk meredakan kecemasan publik.
- 17 November 2022 – *Klarifikasi Kemenkes*: Kemenkes kembali menegaskan bahwa data yang bocor bukan berasal dari sistem internal PeduliLindungi, dan menyatakan bahwa sistem tetap aman dan terlindungi.
- 18 November 2022 – *Pengungkapan dan Validasi*: Kemenkes mengonfirmasi kebocoran data, namun mengklarifikasi bahwa data yang bocor tidak mencakup hasil tes PCR atau diagnosis COVID-19. Pakar keamanan siber mengonfirmasi bahwa data yang bocor valid, meskipun tidak berasal dari sistem resmi PeduliLindungi.
- 22 November 2022 – *Kebocoran Lanjutan oleh Bjorka*: Bjorka kembali membocorkan sampel data yang lebih besar dan mengklaim bahwa data tersebut berasal dari PeduliLindungi. Hal ini memperburuk situasi dan meningkatkan kekhawatiran terkait potensi kebocoran yang lebih luas.
- 23 November 2022 – *Tindak Lanjut oleh Kemenkes dan BSSN*: Kemenkes dan BSSN mengadakan rapat koordinasi untuk melakukan investigasi lebih lanjut mengenai kebocoran data yang diklaim berasal dari PeduliLindungi. BSSN juga mengonfirmasi bahwa mereka tengah melacak asal-usul data yang bocor.
- 24 November 2022 – *Klarifikasi Tambahan oleh Kemenkes*: Kemenkes mengeluarkan pernyataan bahwa data yang bocor tidak mencakup informasi medis atau pribadi yang sensitif, seperti hasil tes PCR atau vaksinasi, dan bahwa data yang bocor lebih banyak terkait dengan informasi administratif.
- 27 November 2022 – *Investigasi Lanjutan*: Pihak kepolisian mulai mengambil bagian dalam penyelidikan untuk menindaklanjuti dugaan kebocoran data yang lebih besar. Bjorka juga dikenal aktif dalam merilis informasi tambahan, namun pihak berwenang belum mengonfirmasi secara jelas asal-usul kebocoran tersebut.
- 30 November 2022 – *Penguatan Keamanan Sistem PeduliLindungi*: Kemenkes bersama dengan BSSN memutuskan untuk memperkuat protokol keamanan pada sistem PeduliLindungi dan melakukan audit sistem untuk memastikan bahwa tidak ada celah atau kerentanan yang memungkinkan kebocoran data lebih lanjut.
- Desember 2022 – *Rilis Laporan Penyidikan*: BSSN dan Kemenkes merilis laporan awal mengenai penyelidikan kebocoran data, yang menjelaskan bahwa data yang bocor kemungkinan berasal dari sumber pihak ketiga atau data replikasi yang terhubung dengan sistem PeduliLindungi, dan bukan dari server utama.

- Januari 2023 – *Perbaikan dan Pemantauan Keamanan*: Kemenkes menyatakan bahwa mereka telah mengambil langkah-langkah untuk mencegah kebocoran serupa di masa depan, termasuk dengan memperbarui sistem keamanan dan memperketat akses data di PeduliLindungi.

Penyebab

Hingga saat ini (berdasarkan informasi terakhir dari sumber yang menjadi rujukan artikel ini), belum ada rilis resmi dari otoritas mengenai penyebab pasti kebocoran data PeduliLindungi. Berikut ini adalah beberapa dugaan penyebab utama.

- Replikasi Data: Data bocor kemungkinan karena adanya replikasi data dari server utama PeduliLindungi ke server replikasi database untuk backup tanpa standar pengamanan yang memadai.
- Celah Keamanan pada Infrastruktur: Adanya celah keamanan pada infrastruktur IT aplikasi PeduliLindungi atau mitra teknologinya yang memungkinkan peretas mengakses data sensitif.
- Serangan Phishing atau Malware: Kemungkinan adanya serangan phishing atau malware yang berhasil mengeksploitasi kredensial staf atau administrator yang memiliki akses ke data, sehingga memungkinkan peretas untuk masuk ke dalam sistem dan mencuri data.
- Kurangnya Pengawasan dan Pengendalian: Pengawasan yang kurang ketat dan pengendalian terhadap sistem keamanan dapat meningkatkan risiko kebocoran data. Hal ini bisa terjadi karena minimnya audit keamanan atau pengujian penetrasi yang tidak rutin dilakukan.

Dampak

Kebocoran data PeduliLindungi menimbulkan kekhawatiran besar bagi jutaan pengguna platform tersebut. Dampak potensial termasuk:

- Potensi Penyalahgunaan Data Pribadi: Data yang bocor dapat digunakan untuk penipuan, pencurian identitas, pelacakan ilegal, dan tujuan jahat lainnya.
- Kerugian Finansial dan Reputasi: Pengguna yang datanya bocor mungkin mengalami kerugian finansial akibat penipuan atau pencurian identitas. Platform PeduliLindungi dan Kementerian Kesehatan juga dapat mengalami kerusakan reputasi.
- Kecemasan dan Stres: Pengguna yang datanya bocor mungkin merasa cemas, stres, dan terancam oleh potensi penyalahgunaan data mereka.
- Ketidakpercayaan terhadap pemerintah dan platform digital: Pengguna mungkin menjadi tidak percaya terhadap pemerintah dan platform digital dalam melindungi data pribadi mereka. Hal ini dapat berdampak pada penggunaan layanan publik dan platform digital di masa depan.

Langkah yang Dilakukan

Untuk mengatasi kebocoran data ini, berbagai pihak telah mengambil langkah-langkah penting. Berikut adalah beberapa tindakan yang telah dilakukan untuk mengatasi masalah ini:

- Investigasi: BSSN, Kemenkes, dan Telkom melakukan investigasi untuk mengidentifikasi sumber kebocoran dan mengambil langkah-langkah pencegahan. Investigasi ini melibatkan

pengecekan sistem, analisis forensik digital, dan penelusuran jejak peretas untuk memastikan penyebab kebocoran.
- Perbaikan Keamanan: Kemenkes dan Telkom telah melakukan perbaikan keamanan pada aplikasi PeduliLindungi dan sistem yang terhubung dengannya. Langkah-langkah ini termasuk memperkuat enkripsi data, memperbarui perangkat lunak, dan meningkatkan protokol keamanan untuk mencegah akses tidak sah di masa depan.
- Pemberitahuan Pengguna: Pengguna PeduliLindungi telah diberitahu tentang kebocoran data dan langkah-langkah yang dapat mereka ambil untuk melindungi diri mereka. Informasi ini mencakup saran untuk mengubah kata sandi, waspada terhadap phishing, dan memantau aktivitas yang mencurigakan pada akun mereka.

Pelajaran yang Dipetik

Kasus kebocoran data PeduliLindungi menjadi pengingat penting tentang pentingnya keamanan data pribadi. Pelajaran yang dapat dipetik dari kasus ini termasuk:
- Pentingnya Memiliki Sistem Keamanan Data yang Kuat: Instansi dan organisasi yang menangani data pribadi harus menerapkan sistem keamanan data yang kuat untuk melindungi data dari akses yang tidak sah.
- Transparansi dan Komunikasi yang Jelas: Instansi dan organisasi yang mengalami kebocoran data harus transparan dan memberikan informasi yang jelas kepada pengguna tentang apa yang terjadi dan langkah-langkah yang diambil untuk mengatasinya.
- Peningkatan Edukasi dan Kesadaran tentang Keamanan Data: Pengguna harus diedukasi tentang pentingnya melindungi data pribadi mereka dan bagaimana mereka dapat melakukannya.
- Perlunya Regulasi yang Lebih Kuat: Pemerintah perlu memperkuat regulasi terkait keamanan data pribadi untuk mencegah kejadian serupa di masa depan.

Sumber

- CNN Indonesia. (2022, November 17). Kemenkes Investigasi Dugaan Kebocoran Data PeduliLindungi oleh Bjorka. CNN Indonesia. Diakses dari www.cnnindonesia.com
- Detik News. (2022, November 17). Heboh Bjorka Bocorkan Data PeduliLindungi, Kemenkes Buka Suara. Detik Health. Diakses dari health.detik.com
- Katadata.co.id. (2022, November 17). Ahli IT: 3,2 Miliar Data PeduliLindungi Dijual Hacker Bjorka Valid. Katadata. Diakses dari katadata.co.id
- Kominfo.go.id. (2021, September). Kemenkes: Tidak Ada Bukti Kebocoran Data di PeduliLindungi. Kominfo. Diakses dari aptika.kominfo.go.id
- Kompas.com. (2022, November 17). Pakar Soroti Pengamanan Data PeduliLindungi yang Dibocorkan Bjorka. Kompas. Diakses dari nasional.kompas.com
- Kompas.com. (2022, November 18). Data PeduliLindungi Bocor, Pemerintah Diminta Tak Saling Lempar Tanggung Jawab. Kompas. Diakses dari nasional.kompas.com

Beberapa contoh insiden kebocoran data ini menunjukkan bahwa kebocoran data kesehatan bukan lagi kejadian langka, melainkan ancaman nyata yang harus ditangani dengan serius. Setiap kasus menyoroti pentingnya penerapan langkah-langkah pencegahan yang lebih efektif yaitu:

- Pengamanan yang lebih ketat, dan kolaborasi yang lebih erat antara pemerintah, institusi kesehatan, khususnya penyedia layanan kesehatan dan penyedia teknologi untuk membangun sistem pelindungan data yang lebih kuat di masa depan.
- Kolaborasi antara sektor publik dan swasta, bersama dengan kebijakan yang mengutamakan pengelolaan data yang transparan dan aman, sangat diperlukan untuk menciptakan ekosistem yang lebih aman.
- Dalam menghadapi ancaman yang terus berkembang, institusi kesehatan harus mengimplementasikan kebijakan keamanan data yang ketat, termasuk penilaian risiko keamanan (SRA) dan penilaian dampak privasi (PIA).
- Pelatihan rutin bagi staf dan pembentukan tim tanggap insiden keamanan (CSIRT atau sejenisnya) yang responsif dan terlatih sangat penting untuk memastikan kesiapan dalam menghadapi potensi kebocoran data.

Untuk melindungi data kesehatan yang begitu berharga, institusi kesehatan juga perlu memperkuat pengamanan sistem TI mereka, dengan fokus pada enkripsi data, autentikasi dua faktor, dan pemantauan berkelanjutan terhadap potensi celah keamanan. Regulasi Indonesia, melalui Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis dan UU Perlindungan Data Pribadi, menegaskan pentingnya perlindungan data pasien secara ketat dalam setiap layanan digital. Selain privasi data, perlindungan hukum juga mencakup hak pasien dalam memperoleh layanan medis yang layak. Hubungan antara dokter dan pasien yang terjalin secara daring tetap harus mematuhi kaidah-kaidah kontrak terapeutik, menjamin persetujuan tindakan medis yang jelas, serta memberikan akses pengaduan bila terjadi pelanggaran hak pasien (Peraturan Menteri Kesehatan RI No. 24 Tahun 2022 Tentang Rekam Medis, 2022). Tantangan utama yang dihadapi tenaga medis adalah risiko tuntutan hukum akibat kesalahan diagnosis, malpraktik, atau kendala komunikasi dalam interaksi digital yang minim tatap muka. Pengaturan khusus seperti Permenkes No. 20 Tahun 2019 tentang Penyelenggaraan Telemedicine dan UU Kesehatan No. 17 Tahun 2023 menjadi acuan penting bagi perlindungan hukum tenaga medis dalam era digitalisasi. Transformasi digital layanan kesehatan juga menuntut peningkatan literasi serta kesiapan infrastruktur, baik bagi pasien maupun penyedia layanan. Banyak fasilitas kesehatan dan pelaku usaha aplikasi kesehatan yang belum sepenuhnya memenuhi standar keamanan serta integrasi sistem yang diwajibkan (Lestari, 2020).

Solusi dan Kewajiban Rumah Sakit

- Perkuat Keamanan Digital: Terapkan enkripsi kuat, autentikasi multi-faktor, dan audit keamanan rutin.
- Pelatihan Staf: Tingkatkan kesadaran staf tentang ancaman siber dan praktik keamanan data.
- Kepatuhan Regulasi: Terapkan UU Perlindungan Data Pribadi (PDP) dan regulasi Kemenkes untuk melindungi data pasien.
- Manajemen Pihak Ketiga: Kontrol ketat jika melibatkan penyedia layanan data eksternal.
- Hak Pasien: Pastikan pasien dapat mengakses dan memperbarui data mereka, serta rumah sakit wajib menjaga kerahasiaan data sesuai hukum.

Penerapan hukum terhadap pencurian data (*data breach*) pasien di rumah sakit di Indonesia melibatkan berbagai peraturan perundang-undangan, terutama Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), serta regulasi khusus di sektor kesehatan. Baik individu pelaku maupun institusi rumah sakit dapat menghadapi sanksi pidana, perdata, dan administratif.

Landasan Hukum Utama

Penerapan hukum dalam kasus pencurian data pasien didasari oleh beberapa regulasi kunci:

- UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP): Ini adalah payung hukum utama yang mengatur pemrosesan data pribadi secara umum di Indonesia. Data kesehatan pasien termasuk dalam kategori "data pribadi yang bersifat spesifik" yang memerlukan perlindungan lebih ketat.
- UU No. 17 Tahun 2023 tentang Kesehatan: Pasal Pasal 276 yang menjamin hak pasien memperoleh informasi pribadi terkait kesehatannya, serta adanya kewajiban fasilitas kesehatan dan tenaga medis menjaga kerahasiaan data.
- Peraturan Menteri Kesehatan (Permenkes) No. 24 Tahun 2022 tentang Rekam Medis: Peraturan ini mengatur secara spesifik mengenai rekam medis elektronik dan kewajiban fasilitas pelayanan kesehatan (fasyankes) untuk menjaga kerahasiaan isinya, bahkan setelah pasien meninggal dunia.
- UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE): Regulasi ini dapat digunakan untuk menjerat pelaku penyalahgunaan data dalam sistem elektronik, termasuk ancaman pidana bagi yang tanpa hak mendistribusikan atau membuat dapat diaksesnya informasi elektronik milik orang lain yang bersifat pribadi (Pasal 30–33: Akses ilegal, intersepsi ilegal, gangguan sistem elektronik dan Pasal 35: Pemalsuan data).
- KUHP Bab Tindak Pidana Siber

Pihak yang Bertanggung Jawab dan Sanksi

Pihak yang bertanggung jawab dapat mencakup individu yang melakukan pencurian data dan/atau rumah sakit sebagai pengendali data.

Tanggung Jawab Individu Pelaku

Individu yang secara sengaja dan melawan hukum memperoleh, mengumpulkan, atau mengungkapkan data pribadi pasien dapat dikenakan sanksi pidana berdasarkan UU PDP dan UU ITE:

- Mengumpulkan data secara melawan hukum: Pidana penjara maksimal 5 tahun dan/atau denda hingga Rp 5 miliar.
- Mengungkapkan data pribadi tanpa persetujuan: Pidana penjara maksimal 4 tahun dan/atau denda hingga Rp 4 miliar.
- Penyalahgunaan data: Pidana penjara maksimal 6 tahun dan/atau denda hingga Rp 6 miliar.

Tanggung Jawab Rumah Sakit (Sebagai Pengendali Data)
Rumah sakit memiliki kewajiban untuk menjaga keamanan data pasien dengan menerapkan sistem keamanan yang aman dan andal. Jika terjadi kebocoran data akibat kelalaian, rumah sakit dapat menghadapi:

- Sanksi Administratif: Berupa teguran tertulis, penghentian sementara kegiatan pemrosesan data, denda administratif, hingga penghapusan data pribadi, sesuai mekanisme di UU PDP.
- Sanksi Pidana Korporasi: Dalam pelanggaran berat, rumah sakit sebagai korporasi dapat dikenakan denda maksimal Rp6 miliar.
- Sanksi Perdata: Pasien yang dirugikan dapat mengajukan gugatan perdata untuk menuntut ganti rugi.
- Kerusakan Reputasi: Rumah sakit juga akan mengalami kerugian non-finansial seperti hilangnya kepercayaan pasien dan mitra

Rumah Sakit wajib menerapkan beberapa langkah penting untuk mencegah kebocoran data pasien, seperti:

- Sistem keamanan berlapis (multi-factor authentication)
- Audit sistem secara berkala
- Pembatasan akses pegawai berdasarkan peran (role-based access)
- Pelatihan keamanan digital bagi seluruh pegawai

Pemerintah memiliki peran dalam penting untuk mencegah kebocoran data pasien:

1. Membuat regulasi yang adaptif terhadap perkembangan teknologi.
2. Memperkuat aparat penegak hukum dalam menangani kejahatan siber.
3. Meningkatkan literasi digital masyarakat.

Masyarakat diharapkan untuk:

- Menggunakan internet secara bijak
- Menjaga data pribadi
- Tidak menyebarkan konten ilegal

Simpulan

Penelitian ini bertujuan untuk menganalisis penerapan dan efektivitas perlindungan hukum terhadap data pribadi pasien dalam layanan kesehatan digital di Indonesia serta mengkaji pertanggungjawaban hukum dalam kasus pencurian atau kebocoran data pasien. Hasil kajian menunjukkan bahwa Indonesia telah memiliki kerangka regulasi yang cukup komprehensif melalui UU Perlindungan Data Pribadi, UU Kesehatan, UU ITE, serta peraturan teknis di bidang rekam medis dan telemedicine. Namun demikian, implementasi regulasi tersebut masih menghadapi tantangan pada aspek kesiapan infrastruktur teknologi, kapasitas sumber daya manusia, serta efektivitas pengawasan dan koordinasi antarinstansi. Studi kasus kebocoran data kesehatan menunjukkan bahwa risiko pelanggaran data bersifat nyata dan sistemik, sehingga perlindungan data pasien harus ditempatkan sebagai bagian integral dari tata kelola layanan kesehatan digital.

Implikasi dari temuan ini menegaskan bahwa perlindungan data pasien bukan sekadar kewajiban administratif, melainkan bentuk pemenuhan hak atas privasi dan keamanan layanan kesehatan. Oleh karena itu, diperlukan penguatan sistem keamanan berlapis, audit dan evaluasi berkala, pembatasan akses berbasis peran, pembentukan tim tanggap insiden siber, serta peningkatan

literasi digital tenaga kesehatan dan masyarakat. Pemerintah perlu memperkuat harmonisasi regulasi dan penegakan hukum untuk meningkatkan kepatuhan serta kepercayaan publik. Untuk penelitian selanjutnya, diperlukan kajian empiris mengenai tingkat kepatuhan fasilitas kesehatan terhadap UU Perlindungan Data Pribadi serta studi komparatif dengan negara lain guna merumuskan model perlindungan data kesehatan yang lebih adaptif terhadap perkembangan teknologi.

Daftar Pustaka

Abdullah, A., & Lala, A. (2024). *Legal implications of data breach cases in Indonesia: Challenges and solutions in the era of personal data protection*. Indonesian Cyber Law Review, 1(2). https://doi.org/10.59261/iclr.v1i2.1

ANTARA News. (2025, August 1). *Laporan IBM sebut AI picu kebocoran data perusahaan yang mahal*.

Antik Pujihastuti, Y., Manggandhi, Y., & Rafika, K. (2025). *The impact of the latest health data privacy regulations on patient information access policies in healthcare service facilities*. Research and Evidence on Knowledge in Administration and Management — Medical Electronic Data and Information Systems, 1(2), 45–55. https://doi.org/10.69855/rekammedis.v1i2.306

Benseghir, M., Zerara, A., Bentria, M., Bendriss, H., & Muhtar, M. H. (2025). *Legal aspects of patient data governance in digital health: A comparative analytical study of UAE and Indonesian legislation*. Journal of Indonesian Legal Studies. https://doi.org/10.15294/jils.v10i2.10025

Bisnis.com. (2025, February 19). *Industri data bisa tembus US$274 miliar, pemerintah diminta perkuat keamanan siber*.

Hanifah, H. N., & Irawati, A. C. (2022). *Urgensi cyber law dalam menjaga privasi pasien di rumah sakit era digital*. ADIL Indonesia Journal. https://doi.org/10.35473/aij.v5i2.3945

Hendra, H., Ravel, R., Firdhaus, N., Kurniawan, M. A., & Platina, G. (2020). *E-health personal data protection in Indonesia*. Jurnal Hukum Kesehatan Indonesia. https://doi.org/10.53337/jhki.v1i02.15

IBM. (2024). *Melonjaknya gangguan pelanggaran data mendorong biaya ke rekor tertinggi*. IBM.

IBM. (2024). *Ransomware kian marak: Tren serangan industri layanan kesehatan 2024* (Doug Bonderud). IBM.

Kompas.id. (2024). *Perlindungan data dan risiko ketidakpatuhan korporasi*. Kompas.id.

Magister, E. S., & Andriana, A. (2023). *Insecurity to consumer data protection in the eHealth sector*. Jurnal Penelitian Hukum De Jure. https://doi.org/10.30641/dejure.2023.V23.115-130

Mandey, A. W. (2025). *Legal analysis of patient privacy violation in electronic medical records and its implications for health data protection in Indonesia*. Jurnal Multidisiplin Sahombu, 5(02), 589–594.

Medcom.id. (2024, September 9). *Kerugian akibat kebocoran data sektor keuangan capai Rp68 miliar*.

Medcom.id. (2025, December 29). *Lawan tren global, biaya kebocoran data di ASEAN justru melonjak*.

Pujihastuti, A. (2025). *Health data privacy and patient access policies in Indonesian healthcare*. Research Journal.

Santhi, N. N. P. P. (2023). *Patient data privacy challenges in electronic health systems: A juridical analysis of medical information protection in Indonesia*. West Science Law and Human Rights. https://doi.org/10.58812/wslhr.v3i01.1577

Satriyo, A. B. (2024). Legal impacts and sanctions of personal data protection. *Journal of Law and Public Policy, 30*(3), 275–290.

Shah, S. M., & Khan, R. A. (2020). *Secondary use of electronic health record: Opportunities and challenges*. arXiv preprint.

Shakil, K. A., Zareen, F. J., Alam, M., Jabin, S., & Singh, A. K. (2017). *BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud*. arXiv preprint.

Situmeang, A., Park, J., Sudirman, L., Silviani, N. Z., & Agustini, S. (2023). *Evaluating data breach notification protocols: Comparative analysis of Indonesia and South Korea*. Lentera Hukum. https://doi.org/10.19184/ejlh.v12i1.47621

Suryanto, D., & Riyanto, S. (2024). *Implementasi UU Perlindungan Data Pribadi dalam industri ritel: Kepatuhan dan dampaknya pada konsumen*. Veritas, 10(1), 121–135.

Thapa, C., & Camtepe, S. (2020). *Precision health data: Requirements, challenges and existing techniques for data security and privacy*. arXiv preprint.

Tinungki, J. P. (2019). *Kewajiban dokter dalam membuat rekam medis menurut UU No. 29 Tahun 2004*. *Lex et Societatis, 7*(5).

Wallis, K. A., Eggleton, K. S., Dovey, S. M., Leitch, S., Cunningham, W. K., & Williamson, M. I. (2018). Research using electronic health records: Balancing confidentiality and public good. *Journal of Primary Health Care, 10*(4), 288–291.

Widjaja, G. (2025). Implementation of patient personal data protection in telemedicine services in Indonesia. *Journal of Health Management and Policy, 18*(1), 150–160.