AKADEMIK E-ISSN 2774-8863
Jurnal Mahasiswa Humanis
Vol. 5, No. 2, Mei 2025

Perlindungan Hukum terhadap Rumah Sakit atas Kebocoran Data Rekam Medik Elektronik yang Dilakukan Oleh Peretas

M. Abdullah Sidiq
Universitas Hang Tuah Surabaya, Surabaya, Indonesia
klandestinsidiq@gmail.com

Submitted: 04th February 2025 | **Edited**: 05th April 2025 | **Issued**: 01st May 2025

Cited on: Sidiq, M. A. (2025). Perlindungan Hukum terhadap Rumah Sakit atas Kebocoran Data Rekam Medik Elektronik yang Dilakukan Oleh Peretas. *AKADEMIK: Jurnal Mahasiswa Humanis, 5*(2), 605-620.

ABSTRACT

Hospitals' and the government's respective responsibilities in the event of a data breach involving patients' electronic health records are the focus of this investigation. Using both statutory and conceptual approaches, the research is normative juridical in nature. The findings indicate that: In the event that a patient's electronic medical record data is leaked, the hospital may face three types of legal responsibility. Firstly, there is civil liability, which allows the patient to sue the hospital for breach of contract or broken promise. Secondly, there is criminal liability, which is based on the principle of error and, if proven guilty, can result in fines and jail time for the hospital administrator. As controllers of patient personal data, hospitals may face administrative consequences such as fines, suspension of operations, termination of access to electronic systems, and/or removal from the PSE list (C. Administrative accountability). There are two aspects to the government's legislative safeguards for hospitals regarding the potential disclosure of patient information in electronic health records: preventative measures and punitive measures. Hospitals are safeguarded by Article 191 of Law No. 17 of 2023 on Health in the preventative protection category, whereas those involved in coercive dispute resolution face fines, sanctions, and jail time.

Keywords: Legal Protection, Data leaks, Electronic Medical Records

PENDAHULUAN

Menyusul terbitnya Peraturan Menteri Kesehatan (PMK) nomor 24 tahun 2022 tentang rekam medis. Peralihan ke catatan kesehatan digital dimulai. Setiap fasilitas pelayanan kesehatan yang disebut Fasyanke diwajibkan oleh undang-undang untuk menggunakan sistem rekam kesehatan elektronik. PMK yang berlaku menawarkan kerangka peraturan untuk memudahkan transisi ke teknologi kesehatan yang merupakan komponen pilar keenam transformasi kesehatan. Kebijakan ini menggantikan PMK nomor 269 tahun 2008 untuk memperhitungkan pergeseran kebijakan sosial, kerangka peraturan, dan lingkungan teknologi (Italiani 2013).

Melindungi privasi pasien merupakan tanggung jawab penting setiap karyawan di rumah sakit. Melindungi privasi rekam medis pasien adalah tanggung jawab bersama setiap karyawan di rumah sakit, mulai dari dokter hingga sekretaris. Mungkin ada konsekuensi bagi pasien dan rumah sakit jika rekam medis tidak disimpan dengan aman (Azhar 2023). Jika informasi kesehatan pribadi pasien jatuh ke tangan yang salah, mudah untuk mengetahui mengapa mereka

mungkin kecewa. Akibatnya, kepercayaan mereka terhadap perlindungan keamanan data rumah sakit telah rusak parah. Mereka mungkin menceritakan tantangan ini kepada orang yang mereka cintai jika mereka merasa sedih(Zians 2023). Masyarakat dan pasien akan kehilangan kepercayaan pada sistem layanan kesehatan secara keseluruhan jika tersiar kabar (Kominfo 2022).

Pelanggaran keamanan apa pun yang melibatkan informasi sensitif pasien di rumah sakit dapat dengan mudah menjadi viral di era internet dan media sosial yang ada di mana-mana (Lalu Anugrah Nugraha et al. 2023). Setelah kejadian seperti ini, orang-orang akan berhenti mempercayai rumah sakit untuk menjaga keamanan informasi pribadi mereka. Ketakutan mereka jika rekam medis mereka dipublikasikan membuat mereka tentu saja ragu untuk mencari pertolongan medis di rumah sakit (Amir 2019). Untuk mendapatkan bantuan, mereka lebih memilih mencari di tempat lain. Peretasan dan penjualan enam juta rekam medis pasien dengan ukuran file lebih dari 720 GB dilaporkan di tekno.kompas.com. Hasil radiografi, CT scan, EKG, rontgen, dan tes Covid-19, serta foto pasien dan informasi pribadi (seperti alamat rumah, tanggal lahir, NIK, dan nomor ponsel), termasuk di antara data yang diekspos. Keamanan data rekam medis mereka memprihatinkan mengingat kuantitas dan sumber data yang diungkapkan berasal dari Kementerian Kesehatan (Apriliyani 2021; Subektianto, Ratna, and Zain 2018; Azhar 2023). Koalisi Advokasi Hak Individu atas Privasi memperhatikan kejadian ini. Menurut Direktur Eksekutif koalisi, ELSAM, Kementerian Kesehatan menangani informasi pribadi pasien COVID-19 sebagai bagian dari sistem informasi kesehatan elektronik (Tim COVID-19 IDAI 2020).

Di Indonesia, norma hukum yang mengatur sebagai payung hukum penggunaan data Pasal 5 dan 6 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan Rekam Medis, serta Peraturan Menteri Nomor 24 Tahun 2022 tentang hal tersebut, menyatakan bahwa pasien (Triwati 2019). Terdapat kebutuhan untuk menetapkan perlindungan hukum bagi rumah sakit sebagai entitas yang bertanggung jawab atas kebocoran Rekam Medis Elektronik, karena undang-undang yang ada saat ini hanya mengatur aspek hukum Rekam Medis Elektronik dan tidak mengatur perlindungannya (Indrasari, Wulandari, and Anjayanti 2021; Kusumah 2022).

LANDASAN TEORI

Perlindungan hukum atas kebocoran data merupakan salah satu topik yang semakin penting di tengah pesatnya perkembangan teknologi informasi. Secara teoritis, perlindungan ini bertujuan untuk menjaga keamanan dan kerahasiaan data pribadi yang dimiliki oleh individu atau organisasi. Kebocoran data terjadi ketika informasi yang seharusnya dijaga kerahasiaannya

jatuh ke tangan yang tidak berwenang, yang dapat merugikan pihak yang bersangkutan, baik dari segi finansial, reputasi, hingga privasi. Oleh karena itu, perlindungan hukum menjadi hal yang esensial untuk memberikan rasa aman kepada masyarakat dan mencegah penyalahgunaan data.

Konsep perlindungan data pribadi dalam hukum melibatkan beberapa prinsip dasar, seperti keabsahan pengumpulan data, transparansi dalam pemrosesan, dan pemberian hak kontrol kepada individu atas data mereka. Di banyak negara, perlindungan data pribadi diatur dalam undang-undang yang memuat hak-hak individu dan kewajiban organisasi dalam menjaga data tersebut. Sebagai contoh, di Uni Eropa, terdapat Regulasi Perlindungan Data Umum (GDPR) yang menetapkan standar tinggi untuk perlindungan data pribadi dan memberikan sanksi yang berat terhadap pelanggaran. Hal serupa juga mulai diadopsi oleh banyak negara di seluruh dunia.

Hasil penelitian terdahulu menunjukkan bahwa meskipun sudah ada regulasi yang mengatur perlindungan data, kebocoran data masih sering terjadi. Penelitian yang dilakukan oleh beberapa ahli hukum dan keamanan siber mengungkapkan bahwa faktor penyebab utama kebocoran data adalah kelemahan dalam sistem keamanan teknologi informasi, kurangnya kesadaran pengguna, serta ketidakpatuhan terhadap peraturan yang ada. Di samping itu, beberapa penelitian juga menunjukkan bahwa meskipun ada regulasi seperti GDPR, implementasi di lapangan seringkali kurang efektif, terutama di negara-negara dengan infrastruktur hukum yang belum memadai.

Penelitian lebih lanjut juga menunjukkan bahwa peran pengawasan dan penegakan hukum sangat penting dalam mengurangi risiko kebocoran data. Beberapa studi mengidentifikasi pentingnya pelatihan kepada pegawai dan peningkatan teknologi enkripsi untuk mengamankan data. Selain itu, penting untuk menciptakan kesadaran di kalangan pengguna tentang pentingnya melindungi data pribadi mereka. Untuk itu, diperlukan kerjasama antara pemerintah, perusahaan, dan masyarakat dalam menciptakan ekosistem yang aman dan terlindungi dari ancaman kebocoran data yang dapat merugikan banyak pihak.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif yang menganalisis penerapan kaidah atau norma hukum positif dengan pendekatan konseptual dan perundang-undangan (Yati Nurhayati, Ifrani, and M. Yasir Said 2021; Ibrahim 2008). Penelitian ini mengkaji peraturan-peraturan yang relevan melalui studi literatur, termasuk undang-undang dan peraturan yang berkaitan dengan praktik kedokteran, perlindungan konsumen, ITE, hak asasi manusia, serta kebijakan terkait kesehatan dan rumah sakit. Bahan hukum yang digunakan meliputi bahan

hukum primer, seperti Undang-Undang Dasar 1945, berbagai undang-undang terkait, serta peraturan menteri, dan bahan hukum sekunder berupa buku, jurnal, dan doktrin hukum. Pendekatan ini bertujuan untuk memahami penerapan hukum dalam konteks teori dan praktik terkait isu-isu perlindungan hukum dalam bidang kesehatan dan teknologi informasi.

HASIL PENELITIAN

Tanggungjawab Hukum Rumah Sakit Akibat Kebocoran Data Pasien Rekam Medik Elektronik

Pelanggaran terhadap keamanan data pribadi, baik disengaja maupun tidak, yang mengakibatkan hilangnya, kerusakan, perubahan, pengungkapan, atau akses tidak sah, dikenal sebagai pelanggaran perlindungan data pribadi, termasuk kebocoran data akibat peretasan (Aviat 2022; Munawaroh 2024). Dalam beberapa tahun terakhir, insiden peretasan data pribadi di Indonesia semakin meningkat, termasuk peretasan kartu peringatan kesehatan elektronik (e-HAC) yang melibatkan data pribadi di sektor perawatan kesehatan, seperti informasi status kesehatan, rekam medis, dan rincian keberangkatan (Meilia, Christianto, and Librianty 2019). Perlindungan data pribadi merupakan bagian dari hak privasi yang dijamin oleh Pasal 28G Ayat 1 UUD 1945, yang mengharuskan penyelenggara sistem elektronik untuk menjaga keamanan data pribadi dan menggunakannya hanya untuk tujuan yang sah (Lalu Anugrah Nugraha et al. 2023; Lestari 2021; Indrasari, Wulandari, and Anjayanti 2021).

Selama masih ada barang yang dapat ditukar dengan uang, maka akan terjadi aktivitas kriminal, dan tren ini semakin nyata dalam skala global. Hal ini tidak lepas dari fakta bahwa akun Kotz digunakan untuk bertransaksi dan menjual data pengguna BPJS Kesehatan (Yulius Don Pratama, Sangking, and Thea Farina 2021). Negara harus menerapkan safeguard untuk menjamin keamanan data (Wan et al. 2022). Fakta bahwa akun Kotz memperoleh akses informasi sensitif pengguna dari BPJS Kesehatan menunjukkan bahwa baik data baru maupun data yang sudah ada tidak dilindungi undang-undang (Wandana, Defit, and Sumijan 2020). Sistem keamanan data yang diterapkan BPJS Kesehatan harus memenuhi standar berikut: Control Objectives for Information Technologies (COBIT) (Wabiser and Singgalen 2022), Security Operation Center (SOC) (Vielberth et al. 2020) yang beroperasi sepanjang waktu, dan sertifikasi ISO 27001. Jika BPJS Kesehatan ingin mengetahui siapa pelaku pembobolan data di fasilitasnya, mereka harus memiliki ikatan yang kuat dengan Badan Siber dan Sandi Negara (BSSN) (Haryanto and Sutra 2023; Andreya 2022; Badan Siber Dan Sandi Negara 2023).

Menyusul kebocoran data 279 juta peserta BPJS pada tahun 2021, industri kesehatan kembali dihadapkan pada kenyataan bahwa pada awal tahun 2022, para peretas masih menganggap keamanan data kesehatan sebagai sasaran empuk (Rahim et al. 2023; Direktorat

Sistem Informasi dan Teknologi 2021). Menurut tekno.kompas.com, dokumen berukuran 720 GB berisi 6 juta catatan pasien bocor dan dijual secara online (Maulida and Utomo 2023). Dokumen tersebut berasal dari server Kementerian Kesehatan (Kemenkes) Republik Indonesia. Data dari rekam medis pasien di beberapa institusi di Indonesia termasuk di antara file yang dicuri. Fokus khusus harus diarahkan pada penguatan langkah-langkah keamanan data kesehatan di Indonesia mengingat besarnya volume data yang terpapar dan fakta bahwa data tersebut berasal dari server milik lembaga pemerintah Indonesia.

Peretas kini semakin sering menargetkan fasilitas kesehatan, termasuk rumah sakit, selain database pemerintah, untuk mencuri informasi sensitif (Zians 2023). Manajemen rumah sakit harus memperkuat sistem perlindungan data kesehatan, karena jika sistem Kementerian Kesehatan tidak diperkuat, peretas yang berhasil menembusnya berpotensi mengakses server rumah sakit (Trivia 2023). Pencurian rekam medis di Indonesia telah meningkat, dengan data yang dicuri sering kali dijual di web gelap, seperti kasus pada 2017 ketika dua rumah sakit nasional diserang ransomware WannaCry, yang menyebabkan penjahat meminta uang tebusan (Dewi 2022). Pada 2020, 233.000 catatan pasien COVID-19 dari Indonesia dijual di RaidForums. Data pribadi pasien, yang mencakup informasi identitas seperti nama, alamat, dan rincian medis, sangat rentan terhadap pencurian ini.

Rumah sakit, baik sebagai entitas maupun individu, bertanggung jawab secara hukum atas pelanggaran privasi pasien dan wajib menangani informasi pribadi dengan hati-hati. Pelanggaran dapat dikenakan sanksi administratif, perdata, atau pidana, mulai dari peringatan, denda, hingga pencabutan izin dan kompensasi, serta hukuman pidana. Sebagai badan hukum, rumah sakit dapat diminta pertanggungjawaban hukum oleh pasien atas kesalahan staf medis. Fasilitas pelayanan kesehatan juga bertanggung jawab atas kesalahan penempatan, kehancuran, perubahan, atau penyalahgunaan rekam medis oleh pihak yang tidak berwenang, sebagaimana diatur dalam Pasal 25 Peraturan Menteri Kesehatan Nomor 24 Tahun 2022. Oleh karena itu, rekam medis elektronik (EMR) yang berhubungan langsung dengan pasien harus disimpan dan dilindungi sesuai dengan standar yang ditetapkan untuk memastikan mutu pelayanan medis (Trivia 2023).

Upaya untuk meningkatkan pemberian layanan kesehatan di Indonesia dapat memanfaatkan rekam medis elektronik, yang mencakup informasi identitas pribadi pasien. Namun masih ada kejadian dimana rekam medis elektronik mengalami kendala sehingga implementasinya gagal. Masih belum ada kerangka hukum yang spesifik dan jelas mengenai rekam medis elektronik berdasarkan persyaratan peraturan perundang-undangan mengenai keaslian data medis. Pengelolaan rekam medis elektronik diatur dengan undang-undang tersendiri, sebagaimana tercantum dalam Pasal 2 ayat (2) Peraturan Menteri Kesehatan Nomor

269 Tahun 2008. Menjamin perlindungan data pasien yang disimpan di rumah sakit merupakan hal yang sangat penting. berkaitan dengan beberapa aspek privasi dan keamanan informasi.

Ada 3 bentuk pertanggungjawaban rumah sakit terhadap kebocoran data pribadi pasien yaitu pertanggungjawaban perdata, pidana, dan administrasi:

1. Pertanggungjawaban Rumah Sakit dalam Hukum Perdata

Hukum perdata, yang berfokus pada tanggung jawab pribadi, mengharuskan pihak yang menyebabkan kerugian untuk memberikan ganti rugi, seperti tercantum dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPer). Jika kecerobohan rumah sakit menyebabkan terungkapnya informasi pribadi pasien, ada korelasi langsung antara kesalahan dan kerugian yang diderita, yang berarti rumah sakit telah melakukan perbuatan melawan hukum. Perbuatan melawan hukum ini mengacu pada tindakan yang menyebabkan kerugian bagi orang lain, sebagaimana dijelaskan dalam Pasal 1365 KUHPerdata (Irianto 2021). Selain itu, Pasal 1367 KUHPerdata juga memberikan dasar hukum bagi pertanggungjawaban rumah sakit di Indonesia, yang menyatakan bahwa seseorang bertanggung jawab atas kerugian yang disebabkan oleh perbuatannya sendiri, perbuatan orang yang menjadi tanggung jawabnya, atau barang yang berada di bawah pengawasannya.

Ketentuan ini kemudian dipertegas di dalam Pasal 1367 (3) Kitab UndangUndang Hukum Perdata yang menyatakan bahwa: “Majikan-majikan dan orang yang mengangkat orang lain untuk mewakili urusan-urusan mereka, adalah bertanggung jawab tentang kerugian yang diterbitkan oleh pelayan-pelayan atau bawahan-bawahan mereka didalam melakukan pekerjaan untuk mana orang-orang ini dipakainya.”

Berdasarkan ketentuan yang ada, rumah sakit bertanggung jawab atas *duty of care*, sarana dan prasarananya, serta personalianya. Sebagai badan hukum dan unit usaha yang kompleks, rumah sakit menghadapi masalah hukum yang beragam, karena pelayanan yang diberikan umumnya bersifat *inspanningsverbintennis*, bukan *resultaatsverbintennis*. Dalam mekanisme hukum perdata, pasien dapat menggugat dokter atas perbuatan melawan hukum, sementara rumah sakit dapat digugat berdasarkan wanprestasi atau perbuatan melawan hukum. Sesuai dengan Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUH Perdata), pasien yang dirugikan dapat menuntut ganti rugi dengan syarat adanya kerugian, kesalahan, hubungan kausal antara kesalahan dan kerugian, serta perbuatan yang melawan hukum (Thegra Tawaris 2017).

2. Pertanggungjawaban Rumah Sakit dalam Hukum Pidana

Di Indonesia, setiap orang yang melakukan kejahatan tunduk pada ketentuan pidana yang tertuang dalam Pasal 2 Kitab Undang-Undang Hukum Pidana (KUHP), yang

mengusung premis "tidak ada kejahatan tanpa kesalahan." Pasal ini menyatakan bahwa siapa pun yang berada di wilayah hukum Indonesia dapat dituntut atas pelanggaran yang dilakukannya. KUHP memberikan hukuman maksimal sembilan bulan penjara bagi dokter atau tenaga kesehatan yang secara melawan hukum membocorkan rahasia kedokteran, sebagaimana diatur dalam Pasal 332 (Kolib 2020). Prinsip "Geen Straf Zonder Schuld" yang berarti "tidak ada hukuman tanpa kesalahan" ditegakkan dalam hukum pidana, sehingga seseorang hanya dapat dimintai pertanggungjawaban jika terbukti bersalah. Meskipun demikian, tanggung jawab pidana tanpa pelanggaran atau kesalahan, yang berlaku untuk korporasi, hanya diterapkan pada subjek hukum manusia (Kolib 2020).

Akuntabilitas institusi layanan kesehatan terhadap data pasien diatur oleh sanksi pidana yang tercantum dalam Pasal 65 dan Pasal 67 Undang-Undang Perlindungan Data Pribadi. Pasal 67 mengatur ketentuan pidana terkait kerugian yang tidak diinginkan oleh pemilik data pribadi akibat pelanggaran hukum. Pasal 68 menyatakan bahwa pemalsuan data pribadi dengan tujuan untuk keuntungan pribadi atau orang lain dapat dikenakan pidana penjara hingga 6 tahun atau denda maksimal Rp 5.000.000.000,00. Ketentuan pidana ini menganut teori pemidanaan relatif atau tujuan (Doel Theorien), yang menekankan pemidanaan untuk mencegah kejahatan dan memberikan efek jera pada pelaku, dengan tujuan memperbaiki sikap pelaku agar tidak mengulangi perbuatan merugikan lainnya.

Apabila tindak pidana sebagaimana disebutkan dalam Pasal 67 dan Pasal 68 dilakukan oleh korporasi atau dalam hal ini merupakan fasilitas pelayanan kesehatan, maka pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau pihak korporasi yang bertanggung jawab. Hal ini disebutkan dalam Pasal 70 Ayat (1) Undang-Undang Perlindungan Data Pribadi, sedangkan Pasal 70 Ayat (2) Undang-Undang Perlindungan Data Pribadi menjelaskan bahwa fasilitas pelayanan kesehatan sebagai korporasi yang mutlak secara keseluruhan hanya dapat dikenakan pidana denda. Sebagaimana disebutkan dalam Pasal70 Ayat (2) ini, fasilitas pelayanan kesehatan dapat dijatuhi pidana tambahan berupa perampasan keuntungan dari hasil tindak pidana, pembekuan seluruh atau sebagian fasilitas pelayanan kesehatan, larangan permanen untuk tetap menjalankan usaha, penutupan seluruh fungsi fasilitas pelayanan kesehatan, pelaksanaan kewajiban akibat dari tindak pidana, pembayaran ganti rugi, pencabutan izin, serta pembubaran fasilitas pelayanan kesehatan.

3. Pertanggungjawaban Rumah Sakit dalam Hukum Administrasi

Pertanggungjawaban rumah sakit dalam aspek hukum administratif terkait dengan kewajiban administratif, khususnya dalam mempekerjakan tenaga kesehatan dan

memenuhi persyaratan administratif yang mendukung pelayanan kesehatan bermutu sesuai standar yang ditetapkan (Sri Siswati, Opcit 2021; Alauddin and Sembiring 2021; M and Sidi 2023). Implikasi hukum administrasi antara rumah sakit dan pasien berkaitan dengan kebijakan atau ketentuan yang harus dipenuhi untuk penyelenggaraan pelayanan yang berkualitas. Selain itu, rumah sakit sebagai pengendali data pribadi pasien diatur dalam Undang-Undang Perlindungan Data Pribadi, di mana Pasal 57 ayat (1) mengatur kewajiban pengendali data dan sanksi administratif jika melanggar. Pasal 35 dan Pasal 36 menegaskan bahwa rumah sakit wajib melindungi dan menjaga kerahasiaan data pribadi pasien, dan jika terjadi kelalaian yang menyebabkan kebocoran data, rumah sakit dapat dikenakan sanksi administratif (Bachri and Nurnaeni 2022).

Undang-Undang Kesehatan, khususnya Pasal 189 Ayat (1), mencantumkan 20 kewajiban rumah sakit, termasuk kewajiban sebagai pengendali data pribadi pasien, seperti memberikan informasi yang benar, jelas, dan jujur tentang hak dan kewajiban pasien (Huruf l), serta menghormati dan melindungi hak-hak pasien (Huruf m). Jika kewajiban ini tidak dipenuhi, rumah sakit dapat dikenakan sanksi administratif sesuai Pasal 189 Ayat (2) (Pemerintah RI 2013). Selain itu, penyelenggara sistem elektronik (PSE) juga memiliki tanggung jawab dalam mengintegrasi sistem TI, mengendalikan keamanan transaksi elektronik, serta melindungi pengguna dan konsumen. PSE diwajibkan memiliki SOP untuk pengelolaan keamanan data dan menginformasikan pelanggaran data. PSE yang gagal memenuhi tanggung jawabnya dapat dikenakan tindakan administratif, seperti teguran tertulis, denda, penghentian operasional, atau penghapusan dari daftar PSE, berdasarkan PP No. 71 Tahun 2019.

Perlindungan Hukum Oleh Pemerintah Terhadap Rumah Sakit Atas Terjadinya Kebocoran Data Pasien Pada Rekam Medik Elektronik

Dalam era digital yang semakin canggih, perlindungan keamanan data telah menjadi prioritas utama di seluruh dunia. Data pribadi, bisnis, dan pemerintah semuanya terancam oleh serangan siber dan pelanggaran keamanan. Dalam konteks ini, pemerintah memainkan peran penting dalam menjaga keamanan data dan memberikan kerangka kerja hukum serta infrastruktur yang diperlukan (Amir 2019). Berikut ini beberapa peran pemerintah dalam menjaga keamanan data pribadi di antaranya, Perumusan dan Penegakan Hukum Keamanan Data, Pengembangan Infrastruktur Keamanan, Kerjasama dengan Swasta dan Lembaga Internasional, Pendidikan dan Pelatihan Keamanan Siber, Perlindungan Data Pribadi,Kesiapan dalam Keadaan Darurat, Pemantauan dan Penyelidikan Serangan Siber, dan Promosi Inovasi Keamanan Siber.

Kementerian Komunikasi dan Informatika (Kemkominfo) berperan penting dalam melindungi data rekam medis elektronik dengan menjadi regulator, fasilitator, dan akselerator transformasi digital di sektor kesehatan. Kemkominfo mendorong adopsi rekam medis elektronik (RME) di fasilitas kesehatan dan mengutamakan perlindungan data yang dikelola oleh Penyelenggara Sistem Elektronik (PSE). Selain itu, Kementerian Kesehatan juga berperan melalui Peraturan Menteri Kesehatan (Permenkes) No. 24 Tahun 2022, yang menetapkan batas waktu penerapan RME di seluruh fasilitas kesehatan Indonesia hingga 31 Desember 2023, dengan menekankan perlindungan data rekam medis pasien (AS Handayani 2023). Data rekam medis, yang termasuk dalam klasifikasi data rahasia, harus diperlakukan secara khusus mengingat kompleksitas dan interoperabilitasnya yang dapat meningkatkan risiko kerawanan siber. Fasilitas kesehatan di Indonesia diharuskan mengadopsi penggunaan RME yang mencakup registrasi pasien, pengisian informasi klinis, penyimpanan, transfer, serta perlindungan data pribadi.

Kementerian Kesehatan (Kemenkes) sedang menjalankan proyek rekam medis elektronik (EMR) melalui platform SATUSEHAT, yang telah terintegrasi dengan lebih dari 100 juta pengguna dan 2.200 fasilitas kesehatan di seluruh Indonesia. Untuk menjamin keamanan data yang disimpan dan dipertukarkan, SATUSEHAT menggunakan cloud terenskripsi. Kemenkes mengambil tiga langkah utama untuk menjaga keamanan data: pertama, mengoptimalkan peran tim tanggap siber atau Computer Security Incident Response Team (Health-CSIRT) di sektor kesehatan, dan meningkatkan standar keamanan yang harus dipatuhi oleh semua pihak yang terlibat dalam ekosistem SATUSEHAT (Halim & Suwandy 2023; Rasiban & Riyadi 2024). Tim Health-CSIRT bekerja 24 jam untuk mitigasi, pencegahan, dan pemulihan insiden keamanan siber di lingkungan Kemenkes dan instansi terkait. Selain itu, Kemenkes telah merampungkan proses sertifikasi SATUSEHAT dengan ISO 27001 dan ISO 27018, yang memastikan pengelolaan dan pengamanan data di sistem informasi kesehatan telah memenuhi standar internasional.

Perlindungan hukum terhadap data pribadi merupakan bagian dari perlindungan hak asasi manusia (HAM), yang bertujuan untuk menjaga privasi seseorang dan memastikan hak-hak individu terlindungi dari pelanggaran. Perlindungan ini diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang mencakup pemrosesan data pribadi seperti pengumpulan, pengolahan, penyimpanan, serta penghapusan atau pemusnahan data. Menurut Phillipus M. Hadjon, perlindungan hukum dapat bersifat preventif dan represif; preventif bertujuan mencegah sengketa dengan hati-hati dalam pengambilan keputusan, sementara represif bertujuan menyelesaikan sengketa yang sudah terjadi, termasuk melalui lembaga peradilan (Alvirnia Nurimani Andraputri and Ruhaeni 2023; Republik Indonesia 2022).

Berdasarkan teori Phillipus M. Hadjon diatas, maka jenis perlindungan hukum yang diberikan oleh pemerintah terhadap rumah sakit yang mengalami kebocoran data pribadi dibagi menjadi 2 bentuk diantaranya: preventif dan represif (Adipuspito 2020).

1. Perlindungan Hukum Preventif

Perlindungan hukum preventif pada dasarnya mengacu pada pencegahan. Tindakan pemerintah didasarkan pada kebebasan bertindak. Perlindungan hukum preventif ini sangat penting karena mendorong atau memotivasi pemerintah untuk tetap berhati-hati dalam mengambil suatu keputusan. Berdasarkan pasal 193 Undang-undang Nomor 17 Tahun 2023 Tentang Kesehatan menyebutkan bahwa: "Rumah Sakit bertanggung jawab secara hukum terhadap semua kerugian yang ditimbulkan atas kelalaian yang ditakukan oleh Sumber Daya Manusia Kesehatan Rumah Sakit".

Dalam hal pasien yang dirugikan atas kebocoran data pribadinya, maka rumah sakit berdasarkan pasal 191 Undang-undang Nomor 17 Tahun 2023 Tentang Kesehatan berhak untuk: "Melakukan kerja sama dengan pihak lain dalam mengembangkan pelayanan, menerima bantuan dari pihak lain sesuai dengan ketentuan peraturan perundang-undangan, dan menggugat pihak yang mengakibatkan kerugian".

Berdasarkan hak rumah sakit diatas, maka jika terjadi serangan cyber yang merugikan pasien dengan diretasnya data pribadi pasien, maka langkah yang bisa dilakukan rumah sakit untuk mengantisipasi dan menangani dugaan kebocoran data pribadi Seperti membentuk tim yang bertugas merespon insiden serangan siber yang terjadi yang mengakibatkan kebocoran data pribadi. Tim itu dapat terdiri dari beberapa divisi di dalam perusahaan/rumah sakit seperti IT, legal, dan humas.

Selanjutnya, rumah sakit sebagai sebuah perusahaan juga wajib membuat kebijakan internal seperti standar operasional prosedur (SOP). Hal ini merupakan mandat Undang Undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi yang mewajibkan perusahaan sebagai pengendali data untuk membuat SOP yang bersifat umum untuk melindungi atau menangani data pribadi ketika terjadi insiden serangan siber yang berakibat kebocoran data pribadi. Perusahaan yang sudah maju, dia mengikuti regulasi UU Pelindungan Data Pribadi dan punya SOP yang sifatnya umum dan khusus, sehingga ketika terjadi insiden (serangan) siber sudah ada langkah yang harus dilakukan.

Selain peraturan diatas, dalam hal rekam medis elektronik, pemerintah kini sudah menerbitkan peraturan Menteri Kesehatan yang menaungi penyelenggaraan rekam medis elektronik yang turut memproses data pribadi milik masyarakat. Rekam medis Elektronik didalamnya terdapat begabagai macam data yang tidak hanya mengenai kesehatan tetapi juga identitas masayrakat Indonesia. Sesuai dengan Pasal 32 Indonesia Nomor 24 Tahun

2022 tentang Rekam Medis dikatakan bahwa isi rekam medis dijaga keraha-siaannya oleh seluruh pihak yang terlibat dalam pelayanan kesehatan di fasilitas pelayanan kesehatan walaupun pasien telah meninggal.

Penyelenggaraan rekam medis elektronik di Indonesia berdasarkan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang rekam medis didasarkan pada Prinsip Keamanan Dan Kerahasiaan Data Dan Informasi. Pada Pasal 29 Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang rekam medis menjelaskan bahwa setiap penyelenggaraan Rekam Medis Elektronik harus memenuhi Prinsip Keamanan Data Dan Informasi, yaitu; Kerahasiaan, Integritas, dan Ketersediaan. Ketiga prinsip inilah yang menjadi dasar atau upaya dari pemerintah untuk melindungi data pribadi dalam penyeleng-garaan rekam medis elektronik. Pada ketiga prinsip tersebut dapat dilihat Hak Akses memegang peranan pen-ting dalam penyelenggaraan Rekam Medis Elektronik. Dalam pasal 30 ayat (1) dan (2) Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis dijelas-kan bahwa Hak akses adalah hak istimewa yang diberikan oleh pimpinan fasilitas kesehatan kepada tenaga kesehatan untuk melalukan pemrosesan data dalam rekam medis secara elektronik sesuai dengan standar prosedur oprasional yang ditetap-kan oleh pimpinan fasilitas pelayanan ke-sehatan dan didalam Pasal 30 Ayat 3 Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis dijelas-kan kalau hak akses yang diberikan adalah hak untuk Pengimputan Data, Perbaikan Data dan Melihat Data.

Langkah preventif berikutnya, memastikan sistem keamanan elektronik yang digunakan untuk memproses dan mengelola data pribadi pasien. Misalnya, mematuhi Peraturan Badan Siber dan Sandi Nasional (BSSN) tentang ISO untuk keamanan informasi. Kemudian, melakukan sosialisasi dan pelatihan pelindungan data pribadi kepada karyawan dan lainnya.

2. Perlindungan Hukum Represif

Data pribadi dalam rekam medis adalah informasi sensitif antara pasien dan fasilitas kesehatan yang harus dijaga kerahasiaannya, diatur ketat oleh peraturan pemerintah untuk melindungi rahasia pasien. Siapa pun yang membuka rekam medis tanpa izin dapat dikenakan sanksi pidana, yang bertujuan untuk menyeimbangkan kewajiban dan larangan serta menegakkan peraturan. Perlindungan hukum represif bertujuan menyelesaikan konflik akibat pelanggaran, dengan sanksi seperti denda, penjara, atau hukuman lainnya sebagai bentuk penegakan hukum. Tujuan dari perlindungan hukum adalah mewujudkan keadilan, kemanfaatan, dan kepastian hukum, serta memastikan setiap orang mendapat perlindungan, baik preventif maupun represif (Republik Indonesia 2022).

Berdasarkan teori perlindungan data represif diatur dalam Pasal 100 ayat (1) dan (2) Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, pelanggaran terhadap ketentuan (antara lain) Pasal 31 dikenai sanksi administratif. Sanksi administratif berupa Teguran tertulis, Denda administratif, Penghentian sementara, Pemutusan akses; dan/atau Dikeluarkan dari daftar.

Selain ketentuan pasal di atas, Pasal 26 ayat (2) Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik mengatur bahwa setiap orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini. Pasal 26 ayat (1) Undang- Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik mengatur bahwa kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan.

Meskipun tidak langsung berkaitan dengan kesehatan, akan tetapi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi juga dinilai mampu menjawab sistem pengamanan data pasien. Pasal. 34 UU tentang PDP mengatur bahwa Pengendali Data Pribadi dapat melakukan tindakan pemrosesan terhadap data pribadi yang bersifat spesifik, yang mana data spesifik tersebut juga mencakup data rekam medis, dengan syarat harus terlebih dahulu melakukan penilaian dampak Perlindungan Data Pribadi.

Undang-Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi, Pasal. 36 mengatur mengenai kewajiban pengendali data pribadi untuk menjaga kerahasiaan data pribadi termasuk rekam medis, dan apabila gagal dalam melaksanakan hal tersebut, maka dapat dikenakan sanksi administrasi berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan Data Pribadi, penghapusan atau pemusnahan Data Pribadi, dan/atau denda administratif (Republik Indonesia 2022).

Berdasarkan larangan yang terdapat pada Pasal 65 Undang-Undang Perlindungan Data Pribadi tersebut, maka dijelaskan ketentuan pidana sebagai dasar dari pertanggungjawaban fasilitas pelayanan kesehatan terhadap data rekam medis elektronik pasien. Perlindungan Hukum represif yang melindungi data pribadi juga diatur dalam Pasal 67. Apabila tindak pidana sebagaimana disebutkan dalam Pasal 67 dan Pasal 68 dilakukan oleh korporasi atau dalam hal ini merupakan fasilitas pelayanan kesehatan, maka pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau pihak korporasi yang bertanggung jawab. Hal ini disebutkan dalam Pasal 70 Ayat (1) Undang-Undang Perlindungan Data Pribadi, sedangkan Pasal 70 Ayat (2) Undang-Undang Perlindungan Data Pribadi menjelaskan bahwa fasilitas pelayanan kesehatan

sebagai korporasi yang mutlak secara keseluruhan hanya dapat dikenakan pidana denda (CSA Teddy Lesmana, Elis, and Hamimah 2022).

Sebagaimana disebutkan dalam Pasal 70 Ayat (2) ini, pemilik aplikasi fasilitas pelayanan kesehatan dapat dijatuhi pidana tambahan berupa perampasan keuntungan dari hasil tindak pidana, pembekuan seluruh atau sebagian fasilitas pelayanan kesehatan, larangan permanen untuk tetap menjalankan usaha, penutupan seluruh fungsi fasilitas pelayanan kesehatan, pelaksanaan kewajiban akibat dari tindak pidana, pembayaran ganti rugi, pencabutan izin, serta pembubaran fasilitas pelayanan kesehatan.

Adapun upaya represif untuk memberikan perlindungan rumah sakit atas dugaan kebocoran data rekam medik elektronik pasien bagi yaitu:

a. Langkah pertama yang harus dilakukan yaitu segera menghentikan kebocoran data pribadi secepatnya. Hal itu bersifat teknis dan harus mendapat respon cepat oleh tim yang sudah dibentuk perusahaan dalam hal ini adalah rumah sakit. Tindakan itu harus dilakukan dengan cepat guna mencegah kebocoran data pribadi agar tidak memberikan dampak yang lebih meluas. Langkah tersebut bisa dilakukan dengan mengunci atau menutup akses, melakukan shutdown, dan lain sebagainya.
b. Melakukan asesmen untuk mengetahui sebab kebocoran, siapa saja yang terdampak, dan melakukan konfirmasi apakah benar terjadi kebocoran atau tidak. Sebab, tak jarang perusahaan tidak mengetahui apakah ada kebocoran data pribadi atau tidak, tapi sudah ada klaim dari peretas dan berbagai pemberitaan di media. Ketika dikonfirmasi benar ada kebocoran data pribadi, perusahaan harus melakukan pemberitahuan kepada subjek data dan pemerintah dalam waktu 3x24 jam.
c. Mengevaluasi kembali peristiwa kebocoran data yang terjadi. Lalu, meningkatkan keamanan sistem elektronik, mengevaluasi SOP, dan efektivitasnya.

KESIMPULAN

Tanggungjawab hukum rumah sakit akibat kebocoran data pasien rekam medik elektronik dibagi menjadi 3 bentuk diantaranya: pertanggungjawaban perdata, pidana, dan administrasi. Dalam pertanggungjawaban perdata, pasien dapat menggugat rumah sakit berdasarkan wanprestasi (ingkar janji), Adapun dalam pertanggungjawaban pidana menganut asas kesalahan, dimana apabila rumah sakit sebagai pengendali data pribadi pasien terbukti melakukan kesalahan/kelalaian yang ditimbulkan dari tenaga medis dan mengakibatkan kerugian pada pasien maka dikenakan sanksi berupa denda dan pidana penjara sesuai pasal 67 UU PDP. Dalam pertanggungjawaban administrasi, rumah sakit sebagai pengendali data pribadi pasien dapat dikenakan sanksi administrasi bila tidak menjalankan tanggung jawabnya yang

mengakibatkan terjadinya kebocoran data pribadi pasien. Perlindungan hukum oleh pemerintah terhadap rumah sakit atas terjadinya kebocoran data pasien pada rekam medik elektronik dibagi menjadi 2 yaitu preventif dan represif. Dalam perlindungan preventif, pemerintah memberikan perlindungan yang tertuang dalam pasal 191 Undang-undang Nomor 17 Tahun 2023 Tentang Kesehatan bahwa langkah yang bisa dilakukan rumah sakit untuk mengantisipasi dan menangani dugaan kebocoran data pribadi yaitu dengan membentuk tim yang bertugas merespon insiden serangan siber yang terjadi yang mengakibatkan kebocoran data pribadi. Adapun perlindungan represif ialah perlindungan yang berfungsi untuk menyelesaikan suatu konflik yang ditimbulkan oleh pelanggaran seperti denda, sanksi, dan penjara. Seperti yang disebutkan dalam pasal 67 ayat 1 dan Pasal 67 ayat 2 Undang-Undang No.27 Tahun 2022 tentang Perlindungan data pribadi.

DAFTAR PUSTAKA

Adipuspito, Indiarto. 2020. "PARADIGMA POSITIVISTIK DALAM ILMU HUKUM: Kritik Terhadap Pandangan Teori Hukum Normatif Di Indonesia." JURNAL HUKUM PROYURIS.

Alauddin, Alauddin, and Eka Sulastri Sembiring. 2021. "Perlindungan Hukum Terhadap Pasien Dalam Pelayanan Medik Di Puskesmas Kabupaten Seluma." Majalah Keadilan.

Alvirnia Nurimani Andraputri, Calizta, and Neni Ruhaeni. 2023. "Penegakan Hukum Terhadap Pelaku Penyalahgunaan Penyebaran Data Pribadi Jurnalis Di Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." Bandung Conference Series: Law Studies. https://doi.org/10.29313/bcsls.v3i1.4960.

Amir, Nabbilah. 2019. "Perlindungan Hukum Kerahasiaan Data Pasien Dalam Rekam Medik Elektronik." Seminar Nasional Paperless Healthcare System In Indonesia.

Andreya, Ericha. 2022. "Antisipasi Bersama Tingkatkan Sistem Dan Cegah Serangan Siber." Ditjen Aplikasi Informatika.

Apriliyani, Sinta. 2021. "Penggunaan Rekam Medis Elektronik Guna Menunjang Efektivitas Pendaftaran Pasien Rawat Jalan Di Klinik Dr. Ranny." Cerdika: Jurnal Ilmiah Indonesia. https://doi.org/10.36418/cerdika.v1i10.209.

AS Handayani. 2023. "Implikasi Permenkes Nomor 24 Tahun 2022 Terhadap Pelaksanaan Rekam Medis Elektronik Melalui Sistim Informasi Puskesmas (Simpus) (Studi Kasus Di Puskesmas Temanggung)." Unika.

Aviat. 2022. "Apakah Rumah Sakit Anda Sudah Menerapkan Proteksi Data Secara Menyeluruh?" Aviat.Id. 2022.

Azhar, Mochamad. 2023. "Bagaimana Kemenkes Melindungi Sistem Perawatan Kesehatan Dari Serangan Siber." Govinsider.Asia. 2023.

Bachri, Syamsul, and Nurnaeni Nurnaeni. 2022. "ANALISIS SANKSI PIDANA MALPRAKTEK DOKTER DALAM PERSPEKTIF HUKUM PIDANA." Jurnal Berita Kesehatan. https://doi.org/10.58294/jbk.v15i1.84.

Badan Siber Dan Sandi Negara. 2023. "BSSN Ungkap Lanskap Keamanan Siber Indonesia Tahun 2022 Untuk Literasi Budaya Keamanan Siber." BSSN (Badan Siber Dan Sandi Negara).

CSA Teddy Lesmana, Eva Elis, and Siti Hamimah. 2022. "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia." Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia. https://doi.org/10.52005/rechten.v3i2.78.

Dewi, Riskha Dora Candra. 2022. "Regulasi Privasi Perlindungan Data Pasien Covid-19." JUMANTIK (Jurnal Ilmiah Penelitian Kesehatan).

Direktorat Sistem Informasi dan Teknologi. 2021. "Merunut Kebocoran Data E-HAC Kemenkes, Dari Kronologi Hingga Hapus Aplikasi." Direktorat Sistem Informasi Dan Teknologi. 2021.

Halim, Fandi, and Riche Suwandy. 2023. "Evaluasi User Engagement Dan User Experience Pada Aplikasi Satu Sehat." Journal of Information System Research (JOSH). https://doi.org/10.47065/josh.v5i1.4346.

Haryanto, Agus, and Satya Muhammad Sutra. 2023. "Upaya Peningkatan Keamanan Siber Indonesia Oleh Badan Siber Dan Sandi Negara (BSSN) Tahun 2017-2020." Global Political Studies Journal. https://doi.org/10.34010/gpsjournal.v7i1.8141.

Ibrahim, Johni. 2008. Teori Dan Metodologi Penelitian Hukum Normatif Cetakan Ketiga. Penerbit Banyu Media Publishing, Malang.

Indrasari, Ferika, Ratna Wulandari, and Dwi Nurul Anjayanti. 2021. "Peran Resep Elektronik Dalam Meningkatkan Medication Safety Pada Proses Peresepan Di RSI Sultan Agung Semarang." JURNAL FARMASI DAN ILMU KEFARMASIAN INDONESIA. https://doi.org/10.20473/jfiki.v7i1si2020.1-6.

Irianto, Febi. 2021. "PERTANGGUNGJAWABAN HUKUM PIDANA RUMAH SAKIT SEBAGAI KORPORASI PELAYANAN KESEHATAN." SOL JUSTICIA. https://doi.org/10.54816/sj.v4i2.459.

Italiani, F. A. 2013. "Pengaruh Gaya Kepemimpinan Transformasional Dan Transaksional Terhadap Kinerja Pegawai Departemen SDM PT. Semen Gresik (Persero) Tbk." BISMA (Bisnis Dan Manajemen) 6 (1): 11–18.

Kolib, Abdul. 2020. "Analisis Yuridis Perbandingan Risiko Medis Dengan Kelalaian Medis." AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam.

Kominfo, Kementerian. 2022. "Kominfo Sosialisasi Adopsi Rekam Medis Elektronik." Aptika.Kominfo.Go.Id. 2022.

Kusumah, Raden Minda. 2022. "Analisa Perbandingan Antara Rekam Medis Elektronik Dan Manual." COMSERVA Indonesian Jurnal of Community Services and Development.

Lalu Anugrah Nugraha, Sutarno Sutarno, Ninis Nugraheni, and Andika Persada Putra. 2023. "Perlindungan Hukum Rumah Sakit Atas Penggunaan Data Pasien Dalam Peresepan Elektronik." Unizar Law Review. https://doi.org/10.36679/ulr.v6i2.45.

Lestari, Rinna Dwi. 2021. "Perlindungan Hukum Bagi Pasien Dalam Telemedicine." Jurnal Cakrawala Informasi. https://doi.org/10.54066/jci.v1i2.150.

M, Dessy Listiawati, and Redyanto Sidi. 2023. "Analisis Yuridis Pertanggungjawaban Dokter Atas Kesalahan Pengisian Rekam Medis Sebagai Suatu Malpraktek Administrasi." Jurnal Ners. https://doi.org/10.31004/jn.v7i1.13293.

Maulida, One, and Hari Utomo. 2023. "Pertanggungjawaban Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan Atas Kebocoran Data Pribadi Pengguna Dalam Perspektif Hukum Pidana." Indonesian Journal of Law and Justice.

Meilia, Putri Dianita Ika, Gilbert Mayer Christianto, and Nurfanida Librianty. 2019. "Buah Simalakama Rekam Medis Elektronik: Manfaat Versus Dilema Etik." Jurnal Etika Kedokteran Indonesia. https://doi.org/10.26880/jeki.v3i2.37.

Munawaroh, Nafiatul. 2024. "Tanggung Jawab Pemerintah Atas Kebocoran Data Pribadi." Ww.Hukumonline.Com. 2024.

Pemerintah RI. 2013. "Undang-Undang Kesehatan." Journal of Chemical Information and Modeling.

Rahim, Abdur, Shifa Alfiah Fajriah, Safara Diniah, Vania Indah Sabilah, and Suryadi Suryadi. 2023. "Implementasi Pengawasan Bagi Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan Ditinjau Dari Hukum Administrasi Negara." JIIP - Jurnal Ilmiah Ilmu Pendidikan. https://doi.org/10.54371/jiip.v6i8.2573.

Rasiban, Rasiban, and Sugeng Riyadi. 2024. "Analisis Sentimen Terhadap Aplikasi Satu Sehat Pada Twitter Menggunakan Algoritma Naive Bayes Dan Support Vector Machine." Jurnal Sains Dan Teknologi. https://doi.org/10.55338/saintek.v5i3.2790.

Republik Indonesia. 2022. Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Ditama Binbangkum - BPK RI.

Sri Siswati, Opcit, Hlm.146-150. 2021. "Pasal 1 Angka 1 Undang - Undang Republik Indonesia Nomor 30 Tahun 1999 Tentang Arbitrase Dan Alternatif Penyelesaian Sengketa (UU Arbitrase Dan Alternatif Penyelesaian Sengketa)." Sri Siswati, Opcit, Hlm.146-150.

Subektianto, Rahmad Adi, Madu Ratna, and Ismaini Zain. 2018. "Analisis Kepuasan Pasien Dan Pelaksana Terhadap Sistem Informasi Manajemen Puskesmas Elektronik (Simpustronik) Di Kabupaten Blitar Menggunakan Regresi Logistik Biner." Inferensi.

Tektona, Rahmadi Indra. 2023. "Kepastian Hukum Pemilik Data Pribadi Dalam Aplikasi Satu Sehat." Jurnal Legislasi Indonesia. https://doi.org/10.54629/jli.v20i1.996.

Thegra Tawaris. 2017. "Tanggung Jawab Menurut Hukum Perdata Rumah Sakit Akibat Kelalaian Tenaga Medis." Jurnal Lex Et Societatis.

Tim COVID-19 IDAI. 2020. "Protokol Tatalaksana Covid-19." 1.

Trivia. 2023. "Peran Pemerintah Dalam Menjaga Keamanan Data." Widyasecurity.Com. 2023.

Triwati, Ani. 2019. "Akses Keadilan Sebagai Perlindungan Hukum Bagi Perempuan Berhadapan Dengan Hukum Dalam Sistem Peradilan Pidana." Hukum Dan Masyarakat Madani. https://doi.org/10.26623/humani.v9i1.1445.

Vielberth, Manfred, Fabian Bohm, Ines Fichtinger, and Gunther Pernul. 2020. "Security Operations Center: A Systematic Study and Open Challenges." IEEE Access.

Wabiser, Yan Dirk, and Yerik Afrianto Singgalen. 2022. "An Evaluation of Control Objective for Information Related Technology (COBIT) 4.0 or 4.1: Systematic Literature Review." Journal of Information Systems and Informatics.

Wan, Zhiyu, James W. Hazel, Ellen Wright Clayton, Yevgeniy Vorobeychik, Murat Kantarcioglu, and Bradley A. Malin. 2022. "Sociotechnical Safeguards for Genomic Data Privacy." Nature Reviews Genetics. https://doi.org/10.1038/s41576-022-00455-y.

Wandana, Jeri, Sarjon Defit, and S Sumijan. 2020. "Klasterisasi Data Rekam Medis Pasien Pengguna Layanan BPJS Kesehatan Menggunakan Metode K-Means." Jurnal Informasi Dan Teknologi. https://doi.org/10.37034/jidt.v2i4.73.

Yati Nurhayati, Ifrani, and M. Yasir Said. 2021. "Metodologi Normatif Dan Empiris Perspektif Ilmu Hukum." Jurnal Penegakan Hukum Indonesia.

Yulius Don Pratama, Sangking, and Thea Farina. 2021. "Perlindungan Hukum Terhadap Pasien BPJS Kesehatan Dalam Mendapatkan Pelayanan Kesehatan Di RSUD Dr. Doris Sylvanus Palangka Raya." Journal of Environment and Management.

Zians. 2023. "Kemkominfo Tekankan Perlindungan Data Rekam Medis Elektronik Yang Dikelola Penyelenggara Sistem Elektronik." Www.Majalahglobalreview.Com. 2023.