E-ISSN: 3031-8521
P-ISSN: 3032-1867
Halaman 2899-2916
Volume 3 Nomor 4 Tahun 2026

Penegakan Sanksi Pidana Atas Kebocoran dan Penyalahgunaan Data Rekam Medis Elektronik Menurut UU Kesehatan dan UU Perlindungan Data Pribadi

Nunu Nurjana[1], Nugraha[2], Wulan Indah Permesti[3], Heriyanto[4]
[1-4]Fakultas Hukum, Universitas Sehati Indonesia, Indonesia
e-mail: heriyanto@usindo.ac.id

Abstrak

Kewajiban rekam medis elektronik di Indonesia telah menimbulkan konflik norma antara Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, yang menempatkan dokumen rekam medis sebagai milik fasilitas pelayanan kesehatan, dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang memidana penyalahgunaan data yang bukan milik pelaku. Batas antara pertanggungjawaban administratif dan pidana karenanya tetap kabur. Penelitian ini bertujuan menyusun kerangka penegakan hukum pidana yang terpadu dengan menggunakan teori perlindungan hukum, asas kesalahan, dan teori nilai dasar hukum Radbruch. Kami melakukan penelitian yuridis normatif doktrinal dengan pendekatan perundang-undangan, konseptual, dan analitis. Kami menganalisis tujuh instrumen hukum primer dan literatur ilmiah yang terbit pada 2020-2026 melalui interpretasi gramatikal, sistematis, dan teleologis. Klausul kepemilikan hanya mencakup rekam elektronik sebagai wadah, sehingga informasi klinis tetap menjadi data pasien dan pihak internal yang menyalahgunakan akses melakukan tindak pidana. Delik memperoleh dan memalsukan data mensyaratkan maksud khusus menguntungkan diri sendiri atau orang lain, sedangkan pengungkapan dan penggunaan tidak mensyaratkannya. Kebocoran akibat serangan siber eksternal hanya menimbulkan sanksi administratif bagi fasilitas pelayanan kesehatan apabila tidak ada kesengajaan. Pertanggungjawaban korporasi menjangkau pengurus, pemegang kendali, dan pemilik manfaat, sedangkan penutupan usaha sesuai bagi vendor teknologi tetapi tidak bagi rumah sakit. Penelitian ini menyumbangkan doktrin kepemilikan terbelah dan batas kondisi kriminalisasi insiden rekam medis. Hasilnya memandu pembentuk undang-undang dan aparat penegak hukum dalam mengklasifikasikan fasilitas pelayanan kesehatan sebagai pengendali data dan memisahkan perkara administratif dari pidana.

Kata kunci: *Rekam Medis Elektronik; Pelindungan Data Pribadi; Konflik Norma; Mens Rea; Pertanggungjawaban Pidana Korporasi.*

Abstract

Mandatory electronic medical records in Indonesia have produced a conflict of norms between Law Number 17 of 2023 on Health, which treats medical record documents as facility property, and Law Number 27 of 2022 on Personal Data Protection, which penalizes misuse of data not belonging to the offender. The boundary between administrative and criminal liability therefore remains unclear. This study aims to construct an integrated criminal enforcement framework using legal protection theory, the principle of culpability, and Radbruch's theory of legal values. We conducted a doctrinal normative study using statutory, conceptual, and analytical approaches. We analyzed seven primary legal instruments and scholarly works published between 2020 and 2026 through grammatical, systematic, and teleological interpretation. The ownership clause covers only the electronic record as a container, so clinical information remains the patient's data and insiders who misuse access commit offenses. Offenses of obtaining and forging data require specific intent to benefit oneself or others, whereas disclosure and use do not. Breaches caused by external cyberattacks expose the health facility only to administrative sanctions absent intent. Corporate liability reaches managers, controllers, and beneficial owners, while business closure fits technology vendors but not hospitals. This study contributes a bifurcated ownership doctrine and boundary conditions for criminalizing medical record incidents. It guides lawmakers and law enforcers in classifying health facilities as data controllers and separating administrative from criminal cases.

Keywords: *Electronic Medical Records; Personal Data Protection; Conflict of Norms; Mens Rea; Corporate Criminal Liability.*

LATAR BELAKANG

Transformasi digital dalam pelayanan kesehatan melalui penerapan Rekam Medis Elektronik (RME) merupakan bagian dari upaya meningkatkan efisiensi, kualitas, dan kesinambungan pelayanan medis. Kewajiban penyelenggaraan RME diatur dalam Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis dan diperkuat melalui Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan. Namun, digitalisasi data kesehatan juga menghadirkan risiko kebocoran, peretasan, dan penyalahgunaan informasi pribadi pasien. Kasus kebocoran data peserta BPJS Kesehatan serta serangan *ransomware* terhadap Pusat Data Nasional Sementara pada 2024 memperlihatkan kerentanan sistem elektronik di Indonesia. Kondisi tersebut menunjukkan adanya tantangan dalam mewujudkan perlindungan data kesehatan, meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) telah mengategorikan informasi kesehatan sebagai data pribadi yang bersifat spesifik.

Persoalan hukum muncul karena terdapat perbedaan konstruksi pengaturan antara rezim hukum kesehatan dan rezim pelindungan data pribadi. Pasal 296 dan Pasal 297 Undang-Undang Nomor 17 Tahun 2023 mengatur kewajiban penyelenggaraan rekam medis serta kepemilikan dokumen rekam medis oleh fasilitas pelayanan kesehatan. Sementara itu, Pasal 4 ayat (2) huruf a UU PDP menempatkan informasi

kesehatan sebagai data pribadi spesifik yang berkaitan dengan hak privasi pasien. Selanjutnya, Pasal 35–37 UU PDP mewajibkan pengendali data pribadi melindungi keamanan dan kerahasiaan data yang diproses. Perbedaan pengaturan tersebut menimbulkan persoalan dalam menentukan tanggung jawab fasilitas pelayanan kesehatan, tenaga medis, tenaga administrasi, dan penyedia sistem teknologi informasi ketika terjadi kebocoran atau penyalahgunaan RME.

Dalam kajian akademik, Seh et al. (2020) menunjukkan bahwa sektor kesehatan memiliki tingkat kerentanan tinggi terhadap kebocoran data karena nilai ekonomi informasi medis dan kompleksitas sistem pengelolaannya. Yeo dan Banfield (2022) menjelaskan bahwa insiden keamanan rekam medis elektronik tidak hanya disebabkan serangan eksternal, tetapi juga dipengaruhi faktor manusia, penyalahgunaan akses internal, dan lemahnya pengawasan organisasi. Citron dan Solove (2022) menegaskan bahwa kebocoran data pribadi dapat menimbulkan kerugian terhadap otonomi, kondisi psikologis, dan kedudukan sosial individu. Sementara itu, Solove (2024) mengingatkan bahwa penerapan regulasi pelindungan data perlu mempertimbangkan tingkat kesalahan pelaku dan risiko nyata agar tidak menimbulkan kriminalisasi yang tidak proporsional.

Persoalan keseimbangan antara aksesibilitas dan perlindungan data kesehatan juga dibahas oleh McGraw dan Mandl (2021) serta Gerke, Minssen, dan Cohen (2020). Keduanya menekankan pentingnya tata kelola data yang memungkinkan pemanfaatan informasi untuk pelayanan medis tanpa mengabaikan keamanan dan akuntabilitas pemrosesan. Bradford et al. (2020) menunjukkan pentingnya pembagian tanggung jawab antara pengendali dan prosesor data, sedangkan Koops (2021) menjelaskan fenomena *function creep*, yaitu pergeseran penggunaan data dari tujuan awal pengumpulan menuju tujuan lain yang tidak sesuai dengan dasar pemrosesan yang sah. Meskipun demikian, kajian terdahulu belum sepenuhnya menjelaskan konstruksi pertanggungjawaban pidana multipihak dalam penyelenggaraan RME berdasarkan hukum positif Indonesia.

Berdasarkan kajian tersebut, terdapat tiga kesenjangan penelitian. Pertama, analisis mengenai UU Kesehatan dan UU PDP masih cenderung dilakukan secara sektoral sehingga hubungan antara kepemilikan dokumen rekam medis oleh fasilitas pelayanan kesehatan dan hak privasi pasien belum dikonstruksikan secara sistematis. Kedua, doktrin hukum kesehatan yang berorientasi pada hubungan dokter dan pasien belum sepenuhnya menjelaskan pertanggungjawaban pidana dalam pengelolaan RME yang melibatkan berbagai pihak, termasuk manajemen fasilitas kesehatan dan vendor teknologi informasi. Ketiga, belum terdapat parameter analitis yang memadai untuk membedakan kegagalan pengamanan yang dikenai sanksi administratif dengan perbuatan yang memenuhi unsur tindak pidana, termasuk mekanisme pembuktiannya melalui forensik digital.

Penelitian ini menggunakan tiga landasan teori. Pertama, Teori Perlindungan Hukum dari Satjipto Rahardjo (2000) dan Philipus M. Hadjon (2009) untuk menganalisis perlindungan preventif dan represif terhadap pasien. Kedua, Teori Pertanggungjawaban Pidana dan Asas Kesalahan dari Moeljatno (2008) untuk menilai unsur perbuatan

melawan hukum dan kesengajaan dalam tindak pidana penyalahgunaan data. Ketiga, Teori Nilai Dasar Hukum Gustav Radbruch (1950), yang dipadukan dengan Teori Faktor Penegakan Hukum Soerjono Soekanto (2014), untuk mengevaluasi keseimbangan kepastian hukum, keadilan, dan kemanfaatan dalam penegakan hukum.

Kebaruan penelitian ini terletak pada tiga konstruksi, yaitu doktrin kepemilikan terbelah (*Bifurcated Ownership Doctrine*) antara dokumen RME dan informasi kesehatan pasien, parameter batas kondisi kriminalisasi insiden RME, serta konstruksi pertanggungjawaban pidana korporasi yang proporsional terhadap fasilitas pelayanan kesehatan sebagai layanan publik esensial.

Berdasarkan uraian tersebut, penelitian ini bertujuan menganalisis harmonisasi pengaturan RME menurut UU Kesehatan dan UU PDP, mengidentifikasi unsur tindak pidana serta batas penerapan sanksi administratif dan pidana, dan merumuskan pertanggungjawaban pidana perseorangan maupun korporasi dalam kasus kebocoran dan penyalahgunaan data RME.

METODE

Penelitian ini menggunakan metode yuridis normatif atau penelitian hukum doktrinal dengan orientasi analisis terhadap norma hukum positif. Metode ini dipilih karena permasalahan penelitian berfokus pada disharmoni peraturan perundang-undangan, ketidakjelasan unsur tindak pidana, serta konstruksi pertanggungjawaban pidana dalam penyelenggaraan RME (Smits, 2017; Taekema, 2018).

Penelitian menggunakan tiga pendekatan. Pertama, pendekatan perundang-undangan (*statute approach*) untuk mengkaji hubungan dan sinkronisasi pengaturan antara UU Kesehatan, UU PDP, peraturan pelaksana, dan peraturan terkait sistem elektronik. Kedua, pendekatan konseptual (*conceptual approach*) untuk menganalisis konsep kepemilikan dokumen rekam medis, hak privasi pasien, pengendali dan prosesor data, serta pertanggungjawaban pidana perseorangan dan korporasi. Ketiga, pendekatan analitis (*analytical approach*) untuk menguji unsur tindak pidana, sifat melawan hukum, kesengajaan, dan atribusi pertanggungjawaban pidana.

Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, UU Nomor 17 Tahun 2023 tentang Kesehatan, UU Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, peraturan mengenai Informasi dan Transaksi Elektronik beserta perubahannya, PP Nomor 28 Tahun 2024, dan Permenkes Nomor 24 Tahun 2022. Bahan hukum sekunder diperoleh dari buku, artikel jurnal ilmiah, dan penelitian terdahulu yang relevan, khususnya publikasi tahun 2020–2026. Bahan hukum tersier berupa kamus dan ensiklopedia hukum digunakan untuk mendukung pemahaman terminologi.

Pengumpulan bahan hukum dilakukan melalui penelusuran Jaringan Dokumentasi dan Informasi Hukum Nasional (JDIHN), basis data peraturan Badan Pemeriksa Keuangan, serta repositori jurnal ilmiah. Literatur dikaji berdasarkan relevansi terhadap keamanan data kesehatan, pelindungan data pribadi, hukum pidana, dan pertanggungjawaban korporasi.

Analisis bahan hukum dilakukan melalui interpretasi gramatikal, sistematis, dan teleologis. Interpretasi gramatikal digunakan untuk memahami makna unsur delik dalam UU PDP. Interpretasi sistematis digunakan untuk menghubungkan ketentuan kepemilikan dokumen rekam medis dalam UU Kesehatan dengan hak subjek data dalam UU PDP. Adapun interpretasi teleologis digunakan untuk menilai tujuan perlindungan hukum dan proporsionalitas penerapan sanksi.

Selanjutnya, penelitian menggunakan konstruksi hukum (*rechtsverfijning*), argumentasi *a contrario*, dan penalaran silogisme deduktif untuk membedakan pelanggaran administratif dan tindak pidana. Analisis juga mempertimbangkan asas *lex specialis derogat legi generali*, *lex superior derogat legi inferiori*, dan *lex posterior derogat legi priori*. Keabsahan argumentasi diperkuat melalui perbandingan bahan hukum primer dan sekunder serta pengujian konsistensi norma yang dianalisis.

HASIL DAN PEMBAHASAN

Rekonstruksi Normatif Dualisme Kepemilikan Dokumen Rekam Medis Elektronik dan Kedaulatan Hak Subjek Data Pribadi Spesifik

Tabel 1. Matriks Pemetaan Norma, Status Keberlakuan, dan Titik Antinomi Pengaturan Rekam Medis Elektronik di Indonesia

No.	Instrumen Hukum & Hierarki	Pasal / Ayat Rujukan	Substansi Norma dan Atribusi Hak/Kewajiban	Status Keberlakuan	Temuan Analisis Normatif (Antinomi / Norma Kabur / Kekosongan)
1.	UU Nomor 17 Tahun 2023 tentang Kesehatan (Undang-Undang)	Pasal 296 ayat (1), ayat (2), dan ayat (5)	Mewajibkan tenaga medis dan tenaga kesehatan membuat rekam medis; membebankan penyelenggaraan rekam medis pada fasilitas pelayanan kesehatan (fasyankes); serta mewajibkan penyimpanan dan penjagaan kerahasiaan.	Berlaku aktif	Menempatkan rekam medis sebagai instrumen administratif-klinis tanpa mendefinisikan kedudukan fasyankes sebagai pengendali data pribadi.
2.	UU Nomor 17 Tahun 2023 tentang Kesehatan (Undang-Undang)	Pasal 297 ayat (1), ayat (2), dan ayat (3)	Menyatakan dokumen rekam medis merupakan milik fasyankes, memberikan hak akses informasi kepada pasien, dan mewajibkan fasyankes	Berlaku aktif	Antinomi Kepemilikan: Klaim hak milik fasyankes atas "dokumen" pada ayat (1) berbenturan dengan frasa "data pribadi yang bukan

			menjaga keamanan, keutuhan, kerahasiaan, serta ketersediaan data.		miliknya" pada Pasal 65 dan Pasal 67 UU PDP.
3.	UU Nomor 17 Tahun 2023 tentang Kesehatan (Undang-Undang)	Pasal 298	Memberikan kewenangan kepada Kementerian Kesehatan untuk mengelola data rekam medis guna pengelolaan data kesehatan nasional (pengumpulan, pengolahan, penyimpanan, transfer, dan pengawasan).	Berlaku aktif	Norma Kabur (*Vague Norm*): Batas kewenangan agregasi dan transfer data ke sistem nasional (SatuSehat) belum menyertakan parameter persetujuan eksplisit atau pengecualian yang sinkron dengan Pasal 20–24 UU PDP.
4.	UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Undang-Undang)	Pasal 4 ayat (2) huruf a, Pasal 35, Pasal 36, dan Pasal 37	Mengkualifikasikan data dan informasi kesehatan sebagai data pribadi spesifik; mewajibkan pengendali data pribadi menyusun langkah teknis operasional pengamanan, menjaga kerahasiaan, dan mengawasi seluruh pihak yang terlibat.	Berlaku aktif	Menempatkan pasien sebagai subjek data pemilik kedaulatan privasi dan fasyankes sebagai pengendali data (*data controller*), namun tidak mengatur rezim khusus rahasia kedokteran.
5.	PP Nomor 28 Tahun 2024 (Peraturan Pemerintah)	Pasal 788 ayat (1) dan ayat (3); Pasal 789	Mewajibkan fasyankes, tenaga medis, tenaga kesehatan, manajemen, petugas pembiayaan, dan pihak lain menyimpan rahasia kesehatan pribadi pasien (identitas, anamnesis, pemeriksaan, diagnosis, tindakan, dan hal lain).	Berlaku aktif	Kekosongan Norma Sanksi: Memperluas subjek wajib simpan rahasia medis ke pihak nonmedis, tetapi tidak merumuskan delik pidana maupun mekanisme atribusi ke UU PDP.

6.	Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis (Peraturan Menteri)	Pasal 2 dan Pasal 3 ayat (1)	Mewajibkan seluruh fasyankes menyelenggarakan RME berbasis digital dan terintegrasi dengan prinsip keamanan, kerahasiaan, keutuhan, dan ketersediaan data.	Berlaku aktif (sepanjang tidak bertentangan dengan UU 17/2023)	Hanya memuat sanksi administratif sektoral (teguran hingga pencabutan akreditasi/izin) dan tidak mengatur koordinasi penyidikan apabila terjadi eksfiltrasi data RME.

Sumber: Bahan hukum primer yang diolah dan dianalisis penulis (2026).

Berdasarkan Tabel 1, hasil analisis Hasil analisis menunjukkan bahwa pengaturan RME di Indonesia berada pada persimpangan dua rezim hukum, yaitu hukum kesehatan dan hukum pelindungan data pribadi. UU Nomor 17 Tahun 2023, PP Nomor 28 Tahun 2024, dan Permenkes Nomor 24 Tahun 2022 mengatur penyelenggaraan rekam medis, sedangkan UU Nomor 27 Tahun 2022 mengatur hak subjek data dan kewajiban pengendali serta prosesor data pribadi.

Permasalahan utama terdapat pada hubungan Pasal 297 ayat (1) UU Kesehatan yang menyatakan bahwa dokumen rekam medis merupakan milik fasilitas pelayanan kesehatan dengan Pasal 65 dan Pasal 67 UU PDP yang mengatur larangan memperoleh, mengungkapkan, dan menggunakan data pribadi yang bukan miliknya secara melawan hukum. Apabila kepemilikan dokumen rekam medis ditafsirkan secara mutlak mencakup seluruh informasi yang terkandung di dalamnya, dapat muncul celah hukum bagi pihak internal fasilitas pelayanan kesehatan untuk membenarkan penyalahgunaan data dengan alasan bahwa dokumen tersebut merupakan milik institusi.

Hasil interpretasi sistematis dan teleologis menunjukkan bahwa kepemilikan dokumen rekam medis harus dibedakan dari hak privasi atas informasi kesehatan pasien. Fasilitas pelayanan kesehatan memiliki hak pengelolaan terhadap dokumen dan sistem penyimpanan RME, sedangkan informasi klinis dan biografis yang terkandung di dalamnya tetap merupakan data pribadi pasien sebagai subjek data.

Konstruksi tersebut disebut sebagai doktrin kepemilikan terbelah (*Bifurcated Ownership Doctrine*), yaitu pemisahan antara kepemilikan administratif dan pengelolaan dokumen RME oleh fasilitas pelayanan kesehatan dengan hak privasi pasien atas substansi informasi kesehatannya.

Selain persoalan kepemilikan, Pasal 788 dan Pasal 789 PP Nomor 28 Tahun 2024 memperluas kewajiban menjaga rahasia kesehatan kepada berbagai pihak yang terlibat dalam penyelenggaraan pelayanan kesehatan. Pihak tersebut mencakup tenaga medis, tenaga kesehatan, manajemen fasilitas pelayanan kesehatan, petugas pembiayaan, tenaga administrasi, pengelola teknologi informasi, dan pihak ketiga penyedia sistem elektronik.

Namun, pembagian kewajiban tersebut perlu dihubungkan dengan konsep pengendali data pribadi (*data controller*) dan prosesor data pribadi (*data processor*) dalam UU PDP. Fasilitas pelayanan kesehatan pada umumnya berperan sebagai

pengendali data karena menentukan tujuan dan kendali pemrosesan data pasien. Sementara itu, vendor teknologi informasi dapat berkedudukan sebagai prosesor apabila memproses data berdasarkan instruksi pengendali.

Dengan demikian, tanggung jawab hukum tidak dapat ditentukan hanya berdasarkan status kepemilikan dokumen, tetapi harus mempertimbangkan kedudukan fungsional setiap pihak dalam pemrosesan data.

Temuan ini sejalan dengan konsep *function creep* yang dikemukakan Koops (2021), yaitu penggunaan data yang awalnya dikumpulkan untuk tujuan tertentu kemudian dialihkan untuk kepentingan lain. Dalam konteks RME, informasi yang dikumpulkan untuk diagnosis dan pelayanan medis dapat disalahgunakan untuk pemasaran, diskriminasi, pemerasan, atau kepentingan komersial lainnya.

McGraw dan Mandl (2021) serta Gerke et al. (2020) juga menekankan pentingnya keseimbangan antara pemanfaatan data kesehatan dan perlindungan privasi. Oleh sebab itu, pengelolaan RME harus didasarkan pada prinsip pembatasan tujuan, keamanan pemrosesan, dan akuntabilitas setiap pihak yang memperoleh akses.

Demarkasi Sanksi Administratif dan Kualifikasi Delik Pidana dalam Kebocoran serta Penyalahgunaan Rekam Medis Elektronik

Tabel 2. Matriks Demarkasi Kualifikasi Pelanggaran Administratif dan Tindak Pidana atas Kebocoran serta Penyalahgunaan Rekam Medis Elektronik

No.	Tipologi Perbuatan dalam Penyelenggaraan RME	Dasar Hukum (UU 27/2022 & UU 17/2023)	Unsur Objektif (*Actus Reus*)	Unsur Subjektif (*Mens Rea*) & Unsur Khusus	Kualifikasi Sanksi & Ancaman Maksimum	Alat Bukti Elektronik Utama (Forensik Digital)
1.	Kegagalan sistem keamanan RME akibat serangan siber eksternal tanpa keterlibatan internal, atau keterlambatan notifikasi insiden > 3 x 24 jam.	Pasal 35–37, Pasal 46 jo. Pasal 57 UU PDP; Pasal 297 ayat (3) UU Kesehatan.	Kelalaian menyusun langkah teknis pengamanan, kegagalan pengawasan, atau tidak menyampaikan pemberitahuan tertulis dalam 3 x 24 jam kepada	Kelalaian administratif / ketidakpatuhan standar tata kelola (*culpa* / *regulatory non-compliance*).	Sanksi Administratif: Peringatan tertulis, penghentian sementara pemrosesan, penghapusan data, dan/atau denda administratif maks. 2% pendapatan tahunan (Pasal 57).	Laporan audit keamanan sistem, dokumen SOP, bukti waktu temuan insiden (*incident timestamp*), dan surat notifikasi.

			pasien dan lembaga.			
2.	Memperoleh atau mengumpulkan data RME secara melawan hukum (peretasan eksternal atau pencurian basis data pasien oleh orang dalam).	Pasal 65 ayat (1) jo. Pasal 67 ayat (1) dan Pasal 69 UU PDP.	Memperoleh atau mengumpulkan data pribadi RME yang bukan miliknya secara melawan hukum.	Dengan sengaja (*dolus*) DAN maksud khusus (*bijzonder opzet*) menguntungkan diri sendiri/orang lain yang dapat mengakibatkan kerugian subjek data.	Pidana Penjara paling lama 5 tahun dan/atau Pidana Denda paling banyak Rp5.000.000.000,00 + pidana tambahan perampasan keuntungan & ganti kerugian.	*Server access log*, *firewall/IDS log*, alamat IP pengakses, riwayat unduhan (*database query/dump log*), dan jejak transaksi penjualan.
3.	Mengungkapkan data RME kepada pihak lain tanpa hak (membocorkan diagnosis/status medis pasien ke publik/media sosial/pihak ketiga).	Pasal 65 ayat (2) jo. Pasal 67 ayat (2) dan Pasal 69 UU PDP; Pasal 788–789 PP 28/2024.	Mengungkapkan data pribadi RME yang bukan miliknya secara melawan hukum (tanpa persetujuan sah atau perintah undang-undang).	Dengan sengaja (*dolus*) dan melawan hukum (tidak mensyaratkan unsur maksud menguntungkan diri sendiri).	Pidana Penjara paling lama 4 tahun dan/atau Pidana Denda paling banyak Rp4.000.000.000,00 + pidana tambahan ganti kerugian.	Tangkapan layar terverifikasi *hash value*, riwayat akun pengguna RME (*user audit trail*), rekaman transmisi elektronik, dan metadata perangkat.
4.	Menggunakan data RME secara melawan hukum (memanfaatkan data penyakit pasien untuk	Pasal 65 ayat (3) jo. Pasal 67 ayat (3) dan Pasal 69 UU PDP.	Menggunakan data pribadi RME yang bukan miliknya secara melawan hukum di	Dengan sengaja (*dolus*) dan melawan hukum.	Pidana Penjara paling lama 5 tahun dan/atau Pidana Denda paling banyak Rp5.000.000.000,00 + pidana	Bukti komunikasi elektronik pemerasan/pemasaran, korelasi basis data RME dengan daftar target kontak, dan mutasi

	penipuan, pemerasan, diskriminasi, atau pemasaran ilegal).		luar tujuan pelayanan kesehatan.		tambahan perampasan keuntungan & ganti kerugian.	rekening keuangan.
5.	Memalsukan atau membuat data RME palsu (memanipulasi identitas atau riwayat medis untuk klaim fiktif atau menyamarkan jejak).	Pasal 66 jo. Pasal 68 dan Pasal 69 UU PDP.	Membuat data pribadi palsu atau memalsukan data pribadi dalam sistem RME.	Dengan sengaja (*dolus*) DAN maksud khusus menguntungkan diri sendiri/orang lain yang dapat mengakibatkan kerugian bagi orang lain.	Pidana Penjara paling lama 6 tahun dan/atau Pidana Denda paling banyak Rp6.000.000.000,00 + pidana tambahan perampasan keuntungan & ganti kerugian.	*Database modification log* (*before-and-after record state*), tanda tangan elektronik/kredensial akun pengubah, dan dokumen klaim pembiayaan.

Sumber: Hasil analisis doktrinal atas UU Nomor 27 Tahun 2022, UU Nomor 17 Tahun 2023, dan PP Nomor 28 Tahun 2024 (2026).

Berdasarkan Hasil analisis terhadap UU PDP menunjukkan adanya dua jalur penegakan hukum, yaitu sanksi administratif dan sanksi pidana. Sanksi administratif diatur antara lain dalam Pasal 46 dan Pasal 57 UU PDP, sedangkan tindak pidana terkait data pribadi diatur dalam Pasal 65–70 UU PDP.

Permasalahan muncul karena istilah kebocoran data tidak secara otomatis menunjukkan terpenuhinya unsur tindak pidana. Kebocoran data merupakan suatu peristiwa faktual yang dapat disebabkan serangan eksternal, kelalaian pengamanan, penyalahgunaan akses internal, ataupun tindakan komersialisasi data secara melawan hukum. Oleh karena itu, setiap peristiwa harus dikualifikasikan berdasarkan perbuatan dan unsur kesalahan pelakunya.

Berdasarkan analisis terhadap ketentuan UU PDP, terdapat empat bentuk perbuatan yang perlu dibedakan.

Pertama, memperoleh atau mengumpulkan data pribadi secara melawan hukum. Pasal 65 ayat (1) juncto Pasal 67 ayat (1) UU PDP mengatur larangan memperoleh atau mengumpulkan data pribadi yang bukan miliknya secara melawan hukum. Penerapan ketentuan ini mensyaratkan pembuktian kesengajaan dan maksud khusus untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi subjek data.

Kedua, mengungkapkan data pribadi tanpa hak. Pasal 65 ayat (2) juncto Pasal 67 ayat (2) UU PDP mengatur larangan mengungkapkan data pribadi yang bukan miliknya secara melawan hukum. Pada bentuk perbuatan ini, unsur yang perlu dibuktikan adalah

kesengajaan dan sifat melawan hukum pengungkapan data. Maksud memperoleh keuntungan tidak dirumuskan sebagai unsur khusus dalam ketentuan tersebut.

Ketiga, menggunakan data pribadi secara melawan hukum. Pasal 65 ayat (3) juncto Pasal 67 ayat (3) UU PDP melarang penggunaan data pribadi yang bukan miliknya secara melawan hukum. Pemanfaatan informasi medis untuk pemerasan, penipuan, diskriminasi, maupun pemasaran tanpa dasar pemrosesan yang sah dapat menjadi objek pemeriksaan pidana apabila unsur deliknya terpenuhi.

Keempat, membuat data pribadi palsu atau memalsukan data pribadi. Pasal 66 juncto Pasal 68 UU PDP mengatur larangan pembuatan atau pemalsuan data pribadi. Perbuatan tersebut dapat terjadi melalui manipulasi identitas maupun riwayat medis untuk kepentingan klaim fiktif atau menyembunyikan tindakan tertentu.

Perbedaan unsur tersebut menunjukkan bahwa tidak seluruh bentuk penyalahgunaan data harus memiliki motif keuntungan finansial. Penegak hukum harus membuktikan unsur subjektif sesuai rumusan masing-masing delik dan tidak boleh menyamakan seluruh bentuk perbuatan.

Di sisi lain, kebocoran RME akibat serangan siber eksternal tidak secara otomatis menjadikan rumah sakit sebagai pelaku tindak pidana. Apabila peretasan dilakukan oleh pihak luar tanpa keterlibatan atau kesengajaan pengelola, peretas dapat dimintai pertanggungjawaban pidana berdasarkan perbuatannya. Sementara itu, fasilitas pelayanan kesehatan dapat dikenai sanksi administratif apabila terbukti lalai memenuhi kewajiban pengamanan data atau tidak melaksanakan pemberitahuan kegagalan pelindungan data sesuai ketentuan Pasal 46 dan Pasal 57 UU PDP.

Pembedaan tersebut sejalan dengan asas *geen straf zonder schuld* atau tidak ada pidana tanpa kesalahan sebagaimana dijelaskan Moeljatno (2008). Kelalaian dalam memperbarui sistem keamanan tidak dapat secara otomatis ditafsirkan sebagai kesengajaan melakukan tindak pidana. Pemidanaan harus didasarkan pada terpenuhinya unsur perbuatan, kesalahan, kemampuan bertanggung jawab, dan tidak adanya alasan penghapus pidana.

Aspek pembuktian juga menjadi bagian penting dalam penegakan hukum. Tindak pidana RME umumnya meninggalkan jejak digital yang dapat berupa *server access log*, alamat IP, riwayat unduhan basis data, *user audit trail*, metadata perangkat, dan catatan perubahan data. Bukti tersebut harus diperiksa melalui prosedur forensik digital dengan memperhatikan integritas dan rantai penguasaan alat bukti (*chain of custody*).

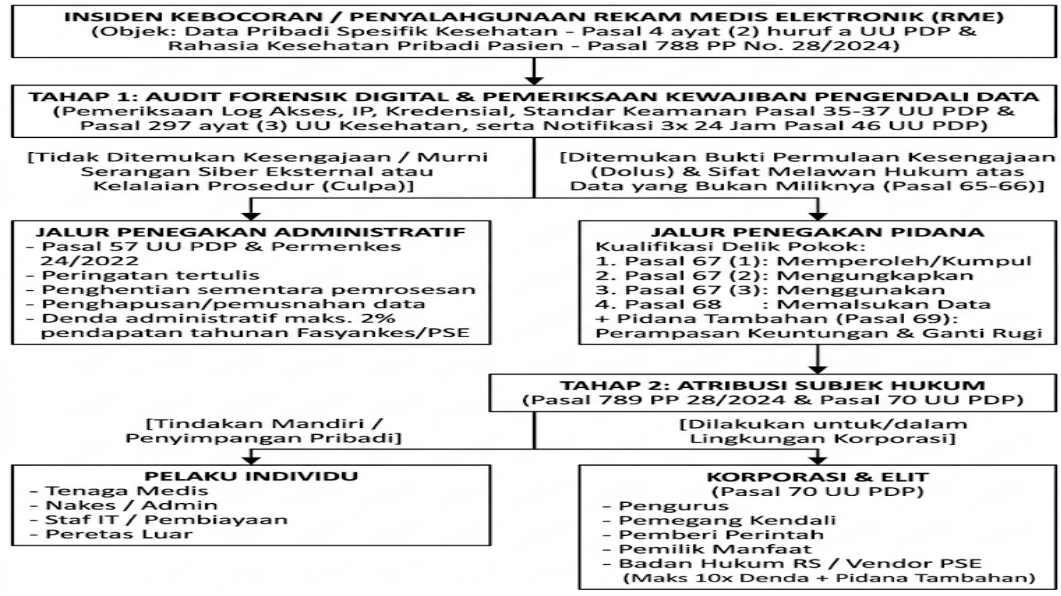
Korelasi antara catatan aktivitas sistem, waktu akses, identitas akun, dan komunikasi elektronik diperlukan untuk menentukan apakah akses dilakukan dalam rangka pelayanan medis yang sah atau merupakan penyalahgunaan kewenangan. Penggunaan akun bersama (*shared credentials*) juga perlu dihindari karena dapat menyulitkan atribusi perbuatan kepada individu tertentu.

Dengan demikian, penegakan hukum pidana atas kebocoran RME harus memperhatikan perbedaan antara kegagalan pengamanan, kelalaian administratif, dan tindakan penyalahgunaan data yang dilakukan secara sengaja.

Konstruksi Pertanggungjawaban Pidana Perseorangan dan Korporasi dalam Ekosistem Penyelenggaraan Rekam Medis Elektronik

Penyelenggaraan RME di fasilitas pelayanan kesehatan modern melibatkan rantai pemrosesan data multipihak yang kompleks, mulai dari tenaga medis, staf penunjang, manajemen rumah sakit sebagai pengendali data, hingga korporasi pihak ketiga penyedia layanan sistem elektronik sebagai prosesor data. Hasil analisis normatif terhadap Pasal 70 Undang-Undang Nomor 27 Tahun 2022 yang dihubungkan dengan Pasal 296–297 UU Kesehatan dan Pasal 789 PP Nomor 28 Tahun 2024 menunjukkan bahwa pertanggungjawaban pidana atas tindak pidana RME tidak hanya membebani pelaku individual di tingkat pelaksana, tetapi juga menjangkau korporasi beserta elit pengendali korporasi.

Pasal 70 ayat (1) UU PDP menetapkan bahwa apabila tindak pidana sebagaimana dimaksud dalam Pasal 67 dan Pasal 68 dilakukan oleh Korporasi, pidana dapat dijatuhkan kepada: (i) pengurus; (ii) pemegang kendali; (iii) pemberi perintah; (iv) pemilik manfaat (*beneficial owner*); dan/atau (v) korporasi itu sendiri. Selanjutnya, Pasal 70 ayat (2) dan ayat (3) mengatur bahwa pidana pokok yang dapat dijatuhkan terhadap korporasi adalah pidana denda paling banyak 10 (sepuluh) kali lipat dari maksimal pidana denda yang diancamkan pada Pasal 67 atau Pasal 68 (yakni mencapai Rp40.000.000.000,00 hingga Rp60.000.000.000,00), ditambah sepuluh jenis pidana tambahan mulai dari perampasan keuntungan, pembekuan seluruh atau sebagian usaha, pelarangan permanen melakukan perbuatan tertentu, penutupan seluruh atau sebagian tempat usaha, pelaksanaan kewajiban yang telah dilalaikan, pembayaran ganti kerugian, hingga pencabutan izin. Untuk memvisualisasikan alur atribusi pertanggungjawaban dan mekanisme pemilahan sanksi secara utuh, Gambar 1 menyajikan arsitektur penegakan hukum terpadu atas insiden kebocoran dan penyalahgunaan RME.



Gambar 1. Arsitektur Penegakan Hukum Terpadu dan Atribusi Pertanggungjawaban atas Kebocoran serta Penyalahgunaan Rekam Medis Elektronik

Sebagaimana ditunjukkan pada Gambar 1 dan dijabarkan lebih lanjut dalam matriks atribusi pada Tabel 3, hasil analisis terhadap struktur organisasi fasilitas pelayanan kesehatan membuktikan bahwa penetapan tersangka tindak pidana RME harus membedakan secara presisi antara kejahatan jabatan individual (*occupational crime*) dan kejahatan korporasi (*corporate crime*).

Tabel 3. Matriks Atribusi Pertanggungjawaban Pidana Perseorangan dan Korporasi dalam Penyelenggaraan Rekam Medis Elektronik

No.	Kategori Subjek Hukum (Pasal 789 PP 28/2024 & UU PDP)	Kedudukan Fungsional dalam Pemrosesan RME	Skenario Perbuatan Melawan Hukum	Konstruksi Atribusi Pertanggungjawaban Pidana	Dasar Hukum Pemidanaan & Proporsionalitas Sanksi
1.	Tenaga Medis, Tenaga Kesehatan, Staf Administrasi, Petugas Pembiayaan, atau Petugas IT Internal.	Pengguna terotorisasi (*Authorized User*) di bawah pengawasan Pengendali Data.	Secara mandiri mengunduh, menjual, membocorkan ke media sosial, atau menggunakan data RME pasien untuk keuntungan pribadi di luar perintah jabatan.	Pertanggungjawaban Perseorangan (*Individual Liability*): Perbuatan melampaui batas kewenangan (*ultra vires* pribadi); korporasi tidak dipidana jika telah menerapkan pengamanan & pengawasan memadai (Pasal 35–37).	Pasal 67 ayat (1), (2), atau (3) atau Pasal 68 jo. Pasal 69 UU PDP (Penjara maks. 4–6 tahun, denda maks. Rp4–6 miliar, perampasan keuntungan & ganti rugi).
2.	Pengurus, Direksi Rumah Sakit, Pemegang Kendali, Pemberi Perintah, atau Pemilik Manfaat (*Beneficial Owner*).	Pengambil kebijakan pada Pengendali Data Pribadi (*Data Controller Decision-Maker*).	Memerintahkan atau menyetujui komersialisasi/transfer basis data RME pasien ke perusahaan farmasi/asuransi/pihak ketiga tanpa dasar pemrosesan yang sah, atau menginstruksikan manipulasi data RME.	Pertanggungjawaban Fungsional Elit Korporasi: Atribusi melalui doktrin *directing mind and will* dan komando fungsional karena memiliki kewenangan mengendalikan pemrosesan dan menikmati manfaat.	Pasal 70 ayat (1) jo. Pasal 67/68 dan Pasal 69 UU PDP (Pidana penjara dan denda dikenakan terhadap pengurus/pemberi perintah/pemilik manfaat secara personal).

3.	Korporasi Fasilitas Pelayanan Kesehatan (Badan Hukum Rumah Sakit/Klinik).	Pengendali Data Pribadi (*Data Controller*) dan pemilik dokumen RME (Pasal 297 ayat (1) UU Kesehatan).	Tindak pidana Pasal 67 atau Pasal 68 dilakukan dalam lingkungan korporasi untuk memberikan keuntungan finansial/operasional bagi rumah sakit atau merupakan kebijakan resmi institusi.	Pertanggungjawaban Pidana Korporasi (*Corporate Criminal Liability*): Kumulasi atau alternatif dengan pengurus; namun pidana tambahan penutupan usaha harus mempertimbangkan kesinambungan layanan kesehatan publik.	Pasal 70 ayat (1), (2), dan (3) UU PDP (Denda maks. 10x lipat [Rp40–60 miliar] + perampasan keuntungan, ganti rugi pasien, dan pelaksanaan kewajiban keamanan).
4.	Korporasi Pihak Ketiga Penyedia Sistem Informasi Kesehatan / Vendor Komputasi Awan (PSE).	Prosesor Data Pribadi (*Data Processor*) atau Pengendali Bersama (*Joint Controller*).	Memanfaatkan akses *backdoor* atau menyalin pangkalan data RME rumah sakit klien untuk dilatih pada model komersial, diperjualbelikan, atau diungkapkan secara melawan hukum.	Pertanggungjawaban Pidana Korporasi Prosesor: Prosesor beralih status memikul beban pidana langsung ketika memproses data melampaui instruksi sah pengendali untuk keuntungan korporasi vendor.	Pasal 70 ayat (1)–(3) jo. Pasal 67/68 UU PDP (Denda maks. 10x lipat, pencabutan izin usaha PSE, pembekuan usaha, dan pembayaran ganti kerugian).

Sumber: Hasil analisis dan konstruksi hukum penulis berdasarkan UU Nomor 27 Tahun 2022, UU Nomor 17 Tahun 2023, dan PP Nomor 28 Tahun 2024 (2026).

Penyelenggaraan RME melibatkan berbagai subjek hukum, mulai dari tenaga medis, tenaga kesehatan, staf administrasi, manajemen fasilitas pelayanan kesehatan, hingga penyedia sistem elektronik. Kompleksitas tersebut mengharuskan penegakan hukum mempertimbangkan peran dan kendali setiap pihak dalam proses pemrosesan data.

Pasal 70 UU PDP mengatur bahwa apabila tindak pidana sebagaimana dimaksud dalam Pasal 67 dan Pasal 68 dilakukan oleh korporasi, pertanggungjawaban dapat dikenakan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat (beneficial owner), dan/atau korporasi itu sendiri.

Dalam konteks tersebut, terdapat empat kelompok subjek yang perlu diperhatikan.

Pertama, tenaga medis, tenaga kesehatan, staf administrasi, petugas pembiayaan, dan petugas teknologi informasi sebagai pengguna sistem RME. Apabila mereka secara mandiri mengunduh, menjual, mengungkapkan, atau menggunakan data

pasien di luar kewenangan dan tanpa dasar hukum, pertanggungjawaban pidana dapat dikenakan secara individual sesuai unsur delik yang terbukti.

Kedua, pengurus, direksi, pemegang kendali, pemberi perintah, dan pemilik manfaat korporasi. Mereka dapat dimintai pertanggungjawaban apabila terbukti memerintahkan, menyetujui, atau mengendalikan kebijakan pemrosesan data yang dilakukan secara melawan hukum. Penentuan tanggung jawab harus memperhatikan kewenangan faktual, keterlibatan, dan manfaat yang diperoleh dari tindakan tersebut.

Ketiga, korporasi fasilitas pelayanan kesehatan sebagai pengendali data pribadi. Korporasi dapat dimintai pertanggungjawaban apabila tindak pidana dilakukan dalam lingkungan korporasi dan memenuhi persyaratan atribusi pertanggungjawaban pidana. Namun, penjatuhan sanksi harus memperhatikan kedudukan rumah sakit sebagai penyedia layanan publik yang menyangkut kepentingan masyarakat luas.

Keempat, korporasi penyedia sistem informasi kesehatan atau vendor komputasi awan. Vendor dapat dimintai pertanggungjawaban apabila menggunakan akses sistem untuk menyalin, memperjualbelikan, atau mengungkapkan data pasien secara melawan hukum di luar instruksi pemrosesan yang sah. Dalam keadaan tersebut, kedudukan vendor tidak dapat semata-mata dilindungi oleh kontrak dengan fasilitas pelayanan kesehatan.

Pasal 70 UU PDP juga mengatur denda korporasi yang dapat mencapai sepuluh kali maksimum denda yang diancamkan terhadap tindak pidana terkait, disertai kemungkinan pidana tambahan. Bentuk pidana tambahan tersebut perlu diterapkan secara proporsional berdasarkan sifat perbuatan, peran korporasi, dan akibat yang ditimbulkan.

Penutupan tempat usaha atau pencabutan izin rumah sakit perlu dipertimbangkan secara hati-hati karena dapat mengganggu kesinambungan pelayanan medis dan merugikan masyarakat. Sebaliknya, terhadap vendor teknologi informasi komersial yang secara sengaja menyalahgunakan data pasien, pembekuan kegiatan usaha atau pencabutan izin dapat menjadi instrumen penegakan hukum yang relevan apabila memenuhi persyaratan hukum.

Temuan ini menunjukkan perlunya membedakan kejahatan individual (occupational crime) dan kejahatan korporasi (corporate crime). Pertanggungjawaban tidak seharusnya hanya dibebankan kepada staf pelaksana tingkat bawah apabila tindakan tersebut merupakan bagian dari kebijakan atau perintah pengurus korporasi.

Dalam perspektif Teori Nilai Dasar Hukum Radbruch (1950), penegakan hukum harus mengintegrasikan kepastian hukum, keadilan, dan kemanfaatan. Kepastian hukum menuntut pembuktian unsur delik secara tepat. Keadilan menuntut pertanggungjawaban pihak yang benar-benar memiliki kendali dan terlibat dalam penyalahgunaan data. Kemanfaatan mengharuskan sanksi dijatuhkan tanpa menghilangkan fungsi sosial fasilitas pelayanan kesehatan.

Dengan demikian, pertanggungjawaban pidana dalam penyelenggaraan RME harus didasarkan pada kendali fungsional, keterlibatan, kesalahan, dan manfaat yang diperoleh, bukan semata-mata kedudukan formal seseorang dalam organisasi.

SIMPULAN

Penelitian ini menjawab bagaimana ketentuan pidana dalam UU Pelindungan Data Pribadi dapat ditegakkan secara pasti dan adil terhadap kebocoran dan penyalahgunaan rekam medis elektronik, dengan simpulan bahwa penegakan tersebut tidak dapat dilakukan secara mekanis, melainkan menuntut konstruksi hukum terpadu antara rezim hukum kesehatan dan rezim pelindungan data pribadi. Temuan menunjukkan adanya antinomi kepemilikan antara dokumen rekam medis milik fasilitas pelayanan kesehatan dan unsur "data pribadi yang bukan miliknya", yang dapat diselesaikan dengan memisahkan kepemilikan wadah dokumen dari hak privasi pasien atas isi informasinya, serta menegaskan bahwa kebocoran akibat serangan siber eksternal tanpa kesengajaan termasuk ranah sanksi administratif, sedangkan perolehan, pengungkapan, penggunaan, dan pemalsuan data secara sengaja merupakan ranah pidana yang atribusinya menjangkau pelaku perseorangan, pengurus, pemegang kendali, dan korporasi. Dengan demikian, penelitian ini memperkaya doktrin hukum kesehatan yang semula bertumpu pada hubungan dokter-pasien melalui doktrin kepemilikan terbelah, parameter batas kondisi kriminalisasi, dan pemidanaan korporasi yang proporsional pada layanan publik esensial. Tesis bahwa kepastian hukum dan keadilan substantif atas rekam medis elektronik hanya tercapai apabila kewajiban menjaga rahasia kesehatan menjadi tolok ukur sifat melawan hukum, dan pertanggungjawaban pidana ditegakkan selektif berdasarkan kesengajaan serta kendali fungsional atas data, pun terkonfirmasi.

DAFTAR PUSTAKA

Buku dan Jurnal Ilmiah

Ameln, F. (2014). *Kapita Selekta Hukum Kedokteran* (Edisi Revisi). Jakarta: Grafikatama Jaya.

Bradford, L., Aboy, M., & Liddell, K. (2020). COVID-19 contact tracing apps: A stress test for privacy, the GDPR, and data protection regimes. *Journal of Law and the Biosciences*, 7(1), lsaa034. https://doi.org/10.1093/jlb/lsaa034

Citron, D. K., & Solove, D. J. (2022). Privacy harms. *Boston University Law Review*, 102(3), 793–863. https://scholarship.law.gwu.edu/faculty_publications/1534/

Epstein, L., & King, G. (2002). The rules of inference. *The University of Chicago Law Review*, 69(1), 1–133. https://doi.org/10.2307/1600349

Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. Dalam A. Bohr & K. Memarzadeh (Ed.), *Artificial Intelligence in Healthcare* (hlm. 295–336). Amsterdam: Academic Press / Elsevier. https://doi.org/10.1016/B978-0-12-818438-7.00012-5

Hadjon, P. M. (2009). *Perlindungan Hukum bagi Rakyat di Indonesia* (Edisi Revisi). Surabaya: Bina Ilmu.

Koeswadji, H. H. (2011). *Hukum dan Masalah Medik*. Surabaya: Airlangga University Press.

Komalawati, V. (2015). *Peranan Informed Consent dalam Transaksi Terapeutik: Persetujuan dalam Hubungan Dokter dan Pasien*. Bandung: Citra Aditya Bakti.

Koops, B. J. (2021). The concept of function creep. *Law, Innovation and Technology*, 13(1), 29–56. https://doi.org/10.1080/17579961.2021.1898299

McGraw, D., & Mandl, K. D. (2021). Privacy protections to encourage use of health-relevant digital data in a learning health system. *npj Digital Medicine*, 4(1), 2. https://doi.org/10.1038/s41746-020-00362-8

Moeljatno. (2008). *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta.

Nasution, B. J. (2016). *Hukum Kesehatan: Pertanggungjawaban Dokter*. Jakarta: Rineka Cipta.

Radbruch, G. (1950). Legal philosophy. Dalam K. Wilk (Ed.), *The Legal Philosophies of Lask, Radbruch, and Dabin* (hlm. 43–224). Cambridge: Harvard University Press.

Rahardjo, S. (2000). *Ilmu Hukum*. Bandung: Citra Aditya Bakti.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare*, 8(2), 133. https://doi.org/10.3390/healthcare8020133

Smits, J. M. (2017). What is legal doctrine? On the aims and methods of legal-dogmatic research. Dalam R. van Gestel, H.-W. Micklitz, & E. L. Rubin (Ed.), *Rethinking Legal Scholarship: A Transatlantic Dialogue* (hlm. 207–228). Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316442906.006

Soekanto, S. (2014). *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Jakarta: Rajawali Pers.

Solove, D. J. (2024). Data is what data does: Regulating based on harm and risk instead of sensitive data. *Northwestern University Law Review*, 118(4), 1081–1138. https://scholarlycommons.law.northwestern.edu/nulr/vol118/iss4/4

Taekema, S. (2018). Theoretical and normative frameworks for legal research: Putting theory into practice. *Law and Method*, 2018, 1–17. https://doi.org/10.5553/REM/.000031

Walters, R., & Novak, M. (2021). *Cyber Security, Artificial Intelligence, Data Protection & the Law*. Singapore: Springer. https://doi.org/10.1007/978-981-16-1665-5

Yeo, L. H., & Banfield, J. (2022). Human factors in electronic health records cybersecurity breach: An exploratory analysis. *Perspectives in Health Information Management*, 19(2), 1i. https://pmc.ncbi.nlm.nih.gov/articles/PMC9123525/

Peraturan Perundang-undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Republik Indonesia tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820).

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842).

Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 105, Tambahan Lembaran Negara Republik Indonesia Nomor 6887).

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905).

Peraturan Pemerintah Nomor 28 Tahun 2024 tentang Peraturan Pelaksanaan Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 135, Tambahan Lembaran Negara Republik Indonesia Nomor 6952).

Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis.