Indo Green Journal
https://idngreen.com/index.php/green

e-ISSN: 3025 – 4574, p-ISSN: 3025 – 2679
Volume 4 Nomor 3 Tahun 2026
Halaman: 690 – 695

RESEARCH ARTICLE

Pertanggungjawaban Pidana Korporasi Terhadap Kebocoran Data Pasien Pada Sistem Informasi Rekam Medis Berdasarkan Undang-Undang Perlindungan Data Pribadi

Yanto Irianto[1], Agustiana[2], Bustaman[3], Yulia Rachmawati[4]
Universitas Nahdlatul Ulama Cirebon, Indonesia

yantoirianto755@gmail.com[1], agustiana@unucirebon.ac.id[2], bustaman@unucirebon.ac.id[3], yuliar0728@gmail.com[4]

Kata Kunci: Pertanggungjawaban Pidana Korporasi, Kebocoran Data, Rekam Medis Elektronik, Pelindungan Data Pribadi, Keamanan Siber

Abstrak

Transformasi digital pada sektor kesehatan telah mendorong penggunaan sistem informasi rekam medis elektronik secara luas di berbagai fasilitas pelayanan kesehatan. Meskipun memberikan manfaat berupa efisiensi dan peningkatan kualitas pelayanan, digitalisasi rekam medis juga meningkatkan risiko kebocoran data pasien yang merupakan data pribadi bersifat spesifik dan memerlukan perlindungan hukum yang lebih ketat. Penelitian ini bertujuan untuk menganalisis konstruksi pertanggungjawaban pidana korporasi terhadap kebocoran data pasien pada sistem informasi rekam medis berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi serta mengkaji tantangan pembuktian kelalaian korporasi dalam proses peradilan pidana. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus. Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier yang dianalisis secara kualitatif melalui metode interpretasi hukum dan argumentasi hukum. Hasil penelitian menunjukkan bahwa UU PDP telah mengakui korporasi sebagai subjek hukum pidana yang dapat dimintai pertanggungjawaban atas kebocoran data pribadi yang terjadi dalam lingkungan korporasi. Pertanggungjawaban pidana korporasi dapat dikonstruksikan melalui teori identifikasi dan konsep kelalaian korporasi, terutama apabila terdapat kegagalan dalam penerapan prinsip keamanan sistem seperti enkripsi data, pengendalian akses, dan audit keamanan informasi. Tantangan utama dalam penegakan hukum terletak pada pembuktian hubungan kausal antara kegagalan pengamanan sistem dengan terjadinya kebocoran data serta pembedaan antara serangan siber yang tidak dapat dihindari dan kelalaian korporasi. Oleh karena itu, integrasi antara hukum pidana dan standar keamanan informasi menjadi penting dalam mewujudkan perlindungan data pasien di era digital.

Keyword: *Corporate Criminal Liability, Data Breach, Electronic Medical Records, Personal Data Protection, Cybersecurity*

Abstract

Digital transformation in the healthcare sector has accelerated the implementation of electronic medical record information systems across healthcare institutions. While digitalization improves efficiency and enhances the quality of healthcare services, it also increases the risk of patient data breaches involving sensitive personal data that require a higher level of legal protection. This study aims to analyze the construction of corporate criminal liability for patient data breaches within electronic medical record systems under Law Number 27 of 2022 concerning Personal Data Protection and to examine the evidentiary challenges in proving corporate negligence in criminal proceedings. This research employs a normative legal research method using statutory, conceptual, and case approaches. The legal materials consist of primary, secondary, and tertiary legal sources, which are analyzed qualitatively through legal interpretation and legal reasoning methods. The findings indicate that the Personal Data Protection Law recognizes corporations as criminal law subjects that may be held liable for personal data breaches occurring within the scope of corporate activities. Corporate criminal liability may be established through identification theory and the concept of corporate negligence, particularly where corporations fail to implement essential security measures such as data encryption, access control mechanisms, and information security audits. The principal challenge in law enforcement lies in establishing a causal relationship between system security failures and data breaches, as well as distinguishing unavoidable cyberattacks from punishable corporate negligence. Therefore, integrating criminal law principles with information security standards is essential to ensuring effective protection of patient data in the digital healthcare era.

Information Production:
© 2026 *by the authors of this article. This work is licensed under an Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)*

PENDAHULUAN

Transformasi digital pada sektor kesehatan telah mendorong percepatan implementasi Sistem Informasi Rekam Medis Elektronik (RME) di berbagai fasilitas pelayanan kesehatan di Indonesia (Tuzzahra dkk., 2026). Digitalisasi rekam medis memberikan berbagai keuntungan berupa efisiensi pelayanan, interoperabilitas data,

e-ISSN: 3025 – 4574
p-ISSN: 3025 – 2679

percepatan pengambilan keputusan klinis, serta peningkatan kualitas layanan kesehatan berbasis data. Implementasi RME juga menjadi bagian dari agenda transformasi sistem kesehatan nasional yang menempatkan data sebagai fondasi utama pelayanan kesehatan modern(Istiqamah, 2025). Namun demikian, peningkatan ketergantungan terhadap sistem digital secara simultan meningkatkan risiko keamanan siber, khususnya terkait kerahasiaan, integritas, dan ketersediaan data pasien.

Data kesehatan merupakan kategori data pribadi yang bersifat spesifik karena memuat informasi mengenai kondisi fisik, mental, riwayat penyakit, tindakan medis, hingga informasi genetika seseorang (Hidayatuloh dkk., 2025). Kebocoran data kesehatan tidak hanya menimbulkan kerugian ekonomi akibat penyalahgunaan identitas, tetapi juga berpotensi menimbulkan diskriminasi sosial, stigma, serta pelanggaran terhadap hak privasi individu yang dijamin secara konstitusional (Mardiyati, 2025). Oleh karena itu, perlindungan terhadap data kesehatan menempati posisi yang lebih tinggi dibandingkan perlindungan terhadap data pribadi pada umumnya (Hadiyantina dkk., 2023). (Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, 2022) secara tegas mengkategorikan data dan informasi kesehatan sebagai data pribadi yang bersifat spesifik sehingga memerlukan tingkat perlindungan yang lebih ketat.

Dalam praktiknya, insiden kebocoran data pasien pada sistem rekam medis elektronik umumnya tidak semata-mata disebabkan oleh serangan siber eksternal, melainkan juga dipicu oleh kegagalan pengamanan sistem yang bersifat internal dan sistemik (Suyahman, 2025). Kerentanan tersebut dapat berupa kelemahan arsitektur backend, kegagalan mekanisme autentikasi dan otorisasi pada API (*Application Programming Interface*), lemahnya sistem enkripsi basis data, kesalahan konfigurasi server, hingga kurangnya penerapan standar keamanan informasi oleh penyelenggara sistem elektronik (Nur dkk., 2024). Berbagai penelitian terbaru menunjukkan bahwa tantangan utama implementasi rekam medis elektronik di Indonesia tidak hanya terletak pada aspek interoperabilitas dan regulasi, tetapi juga pada aspek keamanan data dan tata kelola perlindungan informasi kesehatan pasien (Amalia & Putri, 2026).

Fenomena kebocoran data kesehatan bukan lagi merupakan ancaman hipotetis, melainkan telah menjadi persoalan global yang nyata (Sorisa dkk., 2024). Dalam beberapa tahun terakhir, berbagai insiden kebocoran data kesehatan terjadi pada institusi kesehatan dan penyedia layanan rekam medis digital di berbagai negara akibat serangan ransomware maupun kegagalan pengamanan sistem internal (Nugraha dkk., 2025). Bahkan secara global, sektor kesehatan menjadi salah satu sektor dengan tingkat pertumbuhan insiden kebocoran data tertinggi karena tingginya nilai ekonomi data medis di pasar gelap digital. Indonesia sendiri tidak terlepas dari ancaman tersebut (Sabila & Atman, 2025). Sejumlah laporan mengindikasikan adanya dugaan kebocoran data pasien dan informasi kesehatan yang berasal dari sistem informasi kesehatan nasional maupun fasilitas pelayanan kesehatan (Sidiq, 2025). Kondisi ini menunjukkan bahwa digitalisasi layanan kesehatan tanpa diiringi tata kelola keamanan informasi yang memadai justru dapat menciptakan risiko baru bagi perlindungan hak privasi masyarakat (Safira dkk., 2025).

Dalam perspektif hukum pidana modern, perkembangan teknologi informasi telah mendorong perluasan subjek hukum pidana dari individu menuju korporasi (Margono, 2026). Korporasi sebagai penyelenggara sistem elektronik memiliki kewajiban hukum untuk menjamin keamanan dan kerahasiaan data pribadi yang dikelolanya (Priliasari, 2023). Apabila terjadi kegagalan pengamanan yang mengakibatkan kebocoran data pasien, maka muncul pertanyaan mengenai apakah peristiwa tersebut dapat dikualifikasikan sebagai bentuk kelalaian (*criminal negligence*) atau bahkan kesengajaan (*dolus eventualis*) yang dapat menimbulkan pertanggungjawaban pidana bagi korporasi sebagai pengendali data pribadi (Maharani & Prakoso, 2024).

Pengesahan (Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, 2022) menjadi tonggak penting dalam rezim perlindungan data di Indonesia karena untuk pertama kalinya memberikan dasar normatif yang jelas mengenai pertanggungjawaban pidana korporasi atas pelanggaran data pribadi. (Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, 2022)tidak hanya mengenal sanksi administratif, tetapi juga membuka ruang penerapan sanksi pidana terhadap korporasi yang melakukan pelanggaran, termasuk pemberatan pidana berupa denda berlipat dan pidana tambahan tertentu apabila tindak pidana dilakukan oleh badan hukum atau korporasi.

Meskipun demikian, implementasi pertanggungjawaban pidana korporasi dalam kasus kebocoran data medis masih menghadapi persoalan yuridis dan teknis yang kompleks. Pembuktian unsur kesalahan korporasi memerlukan integrasi antara bukti digital forensik, standar keamanan sistem informasi, audit keamanan siber, serta identifikasi hubungan kausal antara kegagalan pengamanan dengan terjadinya kebocoran data. Kesulitan dalam membuktikan apakah kebocoran terjadi akibat serangan pihak ketiga yang tidak dapat diprediksi atau akibat kelalaian korporasi dalam memenuhi standar keamanan minimum berpotensi menimbulkan impunitas bagi penyelenggara sistem elektronik di sektor kesehatan.

e-ISSN: 3025 – 4574
p-ISSN: 3025 – 2679

Berdasarkan uraian tersebut, penelitian ini menjadi penting untuk mengkaji konstruksi pertanggungjawaban pidana korporasi terhadap kebocoran data pasien pada sistem informasi rekam medis berdasarkan (Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, 2022), sekaligus menganalisis tantangan pembuktian kelalaian korporasi dalam proses peradilan pidana terkait kegagalan pengamanan sistem informasi kesehatan.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif atau doctrinal legal research yang berfokus pada pengkajian norma hukum positif, asas hukum, doktrin, serta konsep hukum yang berkaitan dengan pertanggungjawaban pidana korporasi terhadap kebocoran data pasien pada sistem informasi rekam medis elektronik. Pendekatan normatif dipilih karena penelitian ini bertujuan untuk menganalisis konstruksi pertanggungjawaban pidana korporasi berdasarkan ketentuan peraturan perundang-undangan serta menelaah permasalahan pembuktian unsur kesalahan korporasi dalam tindak pidana pelindungan data pribadi.

Pendekatan penelitian yang digunakan terdiri atas beberapa pendekatan, yaitu pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan dilakukan melalui analisis terhadap berbagai regulasi yang relevan, antara lain (Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, 2022), (Undang-undang (UU) Nomor 17 Tahun 2023 tentang Kesehatan, 2023), (Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, 2024), (Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, 2019), serta (Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis, 2022). Pendekatan konseptual digunakan untuk mengkaji teori pertanggungjawaban pidana korporasi, doktrin *corporate criminal liability*, teori kesalahan (*schuld*), serta konsep kelalaian korporasi (*corporate negligence*) dalam tindak pidana siber. Sementara itu, pendekatan kasus dilakukan melalui telaah terhadap berbagai kasus kebocoran data kesehatan dan insiden keamanan siber pada sektor kesehatan yang relevan dengan objek penelitian.

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang berkaitan dengan pelindungan data pribadi, rekam medis elektronik, dan pertanggungjawaban pidana korporasi. Bahan hukum sekunder terdiri atas buku, artikel jurnal ilmiah, hasil penelitian, doktrin hukum, serta publikasi ilmiah dalam lima tahun terakhir yang membahas keamanan siber sektor kesehatan, perlindungan data pribadi, dan tindak pidana korporasi. Adapun bahan hukum tersier berupa kamus hukum, ensiklopedia hukum, dan sumber referensi lain yang mendukung pemahaman terhadap konsep-konsep yang digunakan dalam penelitian.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan menelusuri berbagai sumber hukum dan literatur ilmiah baik secara konvensional maupun melalui basis data elektronik seperti Google Scholar, Scopus, ScienceDirect, dan portal peraturan perundang-undangan nasional. Seluruh bahan hukum yang diperoleh kemudian diklasifikasikan berdasarkan relevansinya terhadap isu pertanggungjawaban pidana korporasi dan pembuktian kelalaian dalam kasus kebocoran data medis.

Analisis bahan hukum dilakukan secara kualitatif dengan menggunakan metode penafsiran hukum (*legal interpretation*) dan argumentasi hukum (*legal reasoning*). Analisis difokuskan pada identifikasi unsur-unsur pertanggungjawaban pidana korporasi berdasarkan UU PDP, bentuk kesalahan korporasi dalam kegagalan pengamanan sistem informasi rekam medis, serta tantangan pembuktian hubungan kausal antara kelemahan sistem keamanan dengan terjadinya kebocoran data pasien. Hasil analisis kemudian disajikan secara deskriptif-analitis untuk memberikan gambaran yang komprehensif mengenai konstruksi hukum pertanggungjawaban pidana korporasi dalam perlindungan data kesehatan di Indonesia

HASIL DAN PEMBAHASAN

Konstruksi Pertanggungjawaban Pidana Korporasi terhadap Kebocoran Data Pasien Berdasarkan UU PDP

Perkembangan teknologi informasi pada sektor kesehatan telah mengubah paradigma perlindungan hukum terhadap data pasien dari sekadar kewajiban etis profesi medis menjadi kewajiban hukum yang melekat pada penyelenggara sistem elektronik. Dalam konteks penyelenggaraan Sistem Informasi Rekam Medis Elektronik, rumah sakit, klinik, laboratorium kesehatan, maupun perusahaan pengembang aplikasi kesehatan berkedudukan sebagai Pengendali Data Pribadi dan/atau Prosesor Data Pribadi sebagaimana diatur dalam (Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, 2022). Konsekuensi yuridis

e-ISSN: 3025 – 4574
p-ISSN: 3025 – 2679

dari kedudukan tersebut adalah adanya kewajiban untuk menjamin keamanan, kerahasiaan, integritas, dan ketersediaan data pasien yang dikelola dalam sistem elektronik.

Secara dogmatik, (Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, 2022) telah mengadopsi konsep pertanggungjawaban pidana korporasi (*corporate criminal liability*) dengan menempatkan korporasi sebagai subjek hukum pidana yang dapat dimintai pertanggungjawaban atas tindak pidana pelindungan data pribadi. Ketentuan Pasal 69 UU PDP secara eksplisit mengakui kemungkinan penjatuhan pidana terhadap korporasi apabila tindak pidana dilakukan untuk kepentingan korporasi, berdasarkan hubungan kerja, atau dilakukan oleh pihak yang bertindak dalam lingkup kegiatan korporasi. Dengan demikian, pertanggungjawaban pidana tidak lagi terbatas pada pelaku individual seperti administrator sistem, staf teknologi informasi, atau operator data, tetapi dapat ditarik kepada badan hukum yang memperoleh manfaat dari pengelolaan sistem informasi tersebut.

Konstruksi ini sejalan dengan teori identifikasi (*identification theory*) yang memandang tindakan dan kesalahan pejabat senior atau pengambil keputusan strategis sebagai tindakan dan kesalahan korporasi itu sendiri. Dalam praktik pengelolaan sistem rekam medis elektronik, keputusan manajemen rumah sakit untuk tidak mengalokasikan anggaran keamanan siber, tidak melakukan pembaruan sistem keamanan secara berkala, atau mengabaikan rekomendasi audit keamanan informasi dapat dipandang sebagai representasi kehendak korporasi (*corporate mind and will*). Oleh karena itu, apabila keputusan tersebut berkontribusi terhadap terjadinya kebocoran data pasien, unsur kesalahan korporasi dapat dianggap telah terpenuhi.

Selain teori identifikasi, perkembangan hukum pidana korporasi modern juga mengenal penerapan prinsip pertanggungjawaban mutlak (*strict liability*) dalam lingkup tertentu, terutama terhadap pelanggaran yang berkaitan dengan perlindungan kepentingan publik dan keamanan informasi. Dalam rezim perlindungan data pribadi, keberadaan standar keamanan minimum yang wajib dipenuhi oleh pengendali data menyebabkan kegagalan memenuhi standar tersebut dapat menimbulkan tanggung jawab hukum tanpa harus selalu dibuktikan adanya niat jahat secara langsung.

Dalam perspektif hukum pidana, bentuk kesalahan korporasi pada kasus kebocoran data pasien umumnya muncul dalam bentuk kelalaian berat (*culpa lata*). Kelalaian tersebut dapat berupa tidak diterapkannya sistem enkripsi terhadap basis data pasien, tidak adanya mekanisme *Role-Based Access Control* (RBAC), penggunaan kata sandi yang lemah, tidak dilaksanakannya audit keamanan secara berkala, maupun tidak tersedianya sistem deteksi intrusi (*Intrusion Detection System*). Kelalaian tersebut menunjukkan adanya kesadaran korporasi terhadap risiko keamanan yang mungkin terjadi, tetapi risiko tersebut tetap diabaikan karena pertimbangan efisiensi biaya atau alasan operasional lainnya.

Dalam konteks pengembangan perangkat lunak kesehatan, vendor penyedia aplikasi rekam medis elektronik juga memiliki potensi pertanggungjawaban pidana apabila sejak tahap perancangan sistem tidak menerapkan prinsip *security by design* dan *privacy by design*. Sebagai contoh, penyimpanan data pasien dalam format *plaintext*, penggunaan protokol komunikasi yang tidak terenkripsi, atau kegagalan menerapkan mekanisme autentikasi berlapis merupakan bentuk kelalaian teknis yang dapat menjadi dasar atribusi kesalahan kepada korporasi.

UU PDP memberikan konsekuensi hukum yang cukup berat terhadap korporasi yang terbukti melakukan pelanggaran data pribadi. Selain pidana denda yang dapat diperberat hingga sepuluh kali lipat dari ancaman pidana denda terhadap individu, korporasi juga dapat dikenai pidana tambahan berupa perampasan keuntungan yang diperoleh dari tindak pidana, pembekuan sebagian atau seluruh kegiatan usaha, penutupan tempat usaha, pencabutan izin usaha, hingga pembubaran korporasi. Pengaturan tersebut menunjukkan adanya orientasi pembentuk undang-undang untuk menciptakan efek jera sekaligus meningkatkan kepatuhan korporasi dalam pengelolaan data pribadi masyarakat.

Tantangan Pembuktian Kelalaian Korporasi dan Integritas Forensik Sistem dalam Perkara Kebocoran Data Medis

Meskipun (Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, 2022) telah memberikan dasar hukum mengenai pertanggungjawaban pidana korporasi, implementasi norma tersebut dalam praktik peradilan menghadapi tantangan pembuktian yang sangat kompleks. Berbeda dengan tindak pidana konvensional yang umumnya mengandalkan alat bukti fisik dan kesaksian langsung, tindak pidana kebocoran data medis sangat bergantung pada pembuktian digital yang bersifat teknis dan membutuhkan keahlian khusus.

Persoalan utama terletak pada penentuan batas antara serangan siber yang tidak dapat dihindari (*force majeure cyber attack*) dengan kegagalan pengamanan sistem yang seharusnya dapat dicegah oleh korporasi. Tidak setiap insiden kebocoran data secara otomatis menimbulkan pertanggungjawaban pidana bagi

e-ISSN: 3025 – 4574
p-ISSN: 3025 – 2679

pengendali data. Dalam beberapa kondisi, serangan siber dapat dilakukan menggunakan teknik yang sangat canggih sehingga berada di luar kemampuan pengamanan yang wajar dari suatu organisasi.

Namun demikian, apabila hasil investigasi forensik menunjukkan bahwa kebocoran terjadi akibat tidak diterapkannya standar keamanan minimum, maka dalih adanya serangan pihak ketiga tidak dapat digunakan sebagai alasan pembenar maupun alasan pemaaf. Sebagai contoh, penyimpanan basis data pasien dalam bentuk *plaintext* tanpa penerapan algoritma enkripsi seperti AES-256, tidak adanya pembatasan hak akses pengguna, atau penggunaan server tanpa mekanisme pembaruan keamanan secara berkala merupakan indikator kuat adanya kelalaian korporasi dalam memenuhi kewajiban hukum perlindungan data pribadi.

Pembuktian terhadap kelalaian tersebut memerlukan analisis terhadap berbagai artefak digital seperti *server logs*, *access logs*, *audit trails*, metadata transaksi, konfigurasi jaringan, hingga struktur basis data yang digunakan oleh sistem rekam medis elektronik. Melalui analisis forensik digital, penyidik dapat menelusuri apakah terdapat akses yang tidak sah, bagaimana metode eksfiltrasi data dilakukan, serta apakah sistem keamanan yang diterapkan telah memenuhi standar industri yang berlaku.

Dalam praktiknya, korporasi sering kali menggunakan argumentasi bahwa kebocoran data sepenuhnya disebabkan oleh tindakan peretas eksternal (*external threat actor*). Akan tetapi, pendekatan forensik digital modern tidak hanya menilai keberadaan serangan, tetapi juga mengevaluasi tingkat kesiapan dan ketahanan sistem terhadap ancaman tersebut. Apabila ditemukan bahwa sistem tidak memiliki mekanisme enkripsi, autentikasi berlapis, segmentasi jaringan, maupun pencatatan aktivitas pengguna secara memadai, maka kondisi tersebut menunjukkan adanya kegagalan penerapan prinsip *security by design* yang seharusnya telah diimplementasikan sejak tahap pengembangan sistem.

Oleh karena itu, pembuktian unsur kesalahan korporasi dalam perkara kebocoran data medis memerlukan integrasi antara hukum pidana dan standar teknis keamanan informasi. Standar internasional seperti ISO/IEC 27001 mengenai Sistem Manajemen Keamanan Informasi, ISO 27799 mengenai manajemen keamanan informasi kesehatan, serta pedoman keamanan sistem informasi kesehatan yang diterbitkan oleh Kementerian Kesehatan dapat dijadikan parameter objektif untuk menilai apakah korporasi telah memenuhi kewajiban kehati-hatian (*duty of care*) dalam pengelolaan data pasien.

Dengan demikian, ketiadaan fungsi pengamanan yang telah menjadi standar industri tidak lagi dapat dipandang sebagai sekadar kekurangan teknis, melainkan harus dikonstruksikan sebagai bentuk perbuatan melawan hukum secara materiel yang memenuhi unsur kesalahan korporasi. Pendekatan ini penting untuk mencegah terjadinya impunitas korporasi dan memastikan bahwa transformasi digital pada sektor kesehatan berjalan seiring dengan perlindungan hak privasi pasien sebagai hak asasi manusia yang fundamental.

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan mengenai pertanggungjawaban pidana korporasi terhadap kebocoran data pasien pada sistem informasi rekam medis berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, diperoleh beberapa kesimpulan sebagai berikut: 1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mengakui korporasi sebagai subjek hukum pidana yang dapat dimintai pertanggungjawaban atas terjadinya kebocoran data pribadi, termasuk data kesehatan yang merupakan data pribadi bersifat spesifik. Dalam penyelenggaraan sistem informasi rekam medis elektronik, rumah sakit, klinik, maupun perusahaan penyedia layanan teknologi kesehatan berkedudukan sebagai Pengendali Data Pribadi atau Prosesor Data Pribadi yang memiliki kewajiban hukum untuk menjamin keamanan dan kerahasiaan data pasien. Pertanggungjawaban pidana korporasi dapat dikonstruksikan melalui teori identifikasi (*identification theory*) maupun konsep pertanggungjawaban pidana korporasi modern apabila tindak pidana dilakukan oleh pihak yang bertindak dalam lingkungan korporasi atau untuk kepentingan korporasi. Kelalaian dalam menyediakan anggaran keamanan siber, tidak diterapkannya prinsip *security by design*, ketiadaan mekanisme enkripsi, maupun lemahnya pengendalian akses merupakan bentuk kesalahan korporasi yang dapat dikualifikasikan sebagai kelalaian berat (*culpa lata*) dan menjadi dasar penjatuhan sanksi pidana sebagaimana diatur dalam UU PDP; 2) Tantangan utama dalam penegakan hukum terhadap kebocoran data medis terletak pada pembuktian unsur kesalahan korporasi dan hubungan kausal antara kegagalan pengamanan sistem dengan terjadinya kebocoran data. Aparat penegak hukum harus mampu membedakan antara serangan siber yang benar-benar tidak dapat dihindari dengan kelalaian korporasi dalam memenuhi standar keamanan yang semestinya diterapkan. Pembuktian tersebut memerlukan dukungan forensik digital melalui analisis *server logs*, *access logs*, *audit trails*, konfigurasi sistem, dan struktur basis data. Standar keamanan informasi seperti ISO/IEC 27001, ISO 27799, serta pedoman keamanan sistem informasi kesehatan dapat digunakan sebagai parameter objektif untuk menilai terpenuhi atau tidaknya kewajiban kehati-hatian korporasi. Oleh karena itu, integrasi antara pendekatan hukum pidana dan standar

e-ISSN: 3025 – 4574
p-ISSN: 3025 – 2679

teknis keamanan siber menjadi prasyarat penting dalam mewujudkan efektivitas pertanggungjawaban pidana korporasi serta memberikan perlindungan hukum yang optimal terhadap data pribadi pasien di era transformasi digital sektor kesehatan.

DAFTAR REFERENSI

Amalia, A., & Putri, dr S. A. (2026). *Rekam Medis Elektronik (RME): Transformasi Digital dalam Dokumentasi Dan Pelayanan Kesehatan*. Afdan Rojabi Publisher.

Hadiyantina, S., Ayub, Z. A., Cahyandari, D., Paramitha, A. A., Ambarwati, S. D., Mustofa, Y., Sudjati, X. Q. D., & Rahmatika, N. A. (2023). *Perlindungan Data Pribadi dalam Bidang Rekam Medis*. Universitas Brawijaya Press.

Hidayatuloh, C., Sedarmayanti, S., & Utoyo, W. (2025). Analisis Sistem Informasi Manajemen Rumah Sakit (SIMRS) Terhadap Peningkatan Layanan Kesehatan Dalam Mendukung Implementasi Rekam Medis Elektronik Di Era Digital. *Innovative: Journal Of Social Science Research*, *5*(4), 11285–11303. https://doi.org/10.31004/innovative.v5i4.21178

Istiqamah, N. F. (2025). Evaluasi Peran Rekam Medis Elektronik dalam Meningkatkan Kualitas Layanan Kesehatan dan Kepuasan Pasien: Literatur Review. *Graha Medika Public Health Journal*, *4*(1), 14–23.

Maharani, R., & Prakoso, A. L. (2024). Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital. *JURNAL USM LAW REVIEW*, *7*(1), 333–347. https://doi.org/10.26623/julr.v7i1.8705

Mardiyati, S. (2025). Konstitusionalitas Perlindungan Data Pribadi sebagai Bagian dari Hak atas Rasa Aman. *Consensus: Jurnal Ilmu Hukum*, *4*(2), 221–233.

Margono, R. (2026). *Penerapan SEMA No. 13 Tahun 2016: Kompas Jaksa dalam Menjerat Korporasi sebagai Subjek Hukum*. Profesor Rudi Margono.

Nugraha, D. A., Nurfitroh, R., Ul-Haq, N. D., Dika, R. P., & Lagontang, S. N. (2025). Kebocoran Data Bpjs Kesehatan: Ancaman Terhadap Keamanan Informasi Publik Di Era Digital. *Integrative Perspectives of Social and Science Journal*, *2*(03 Juli), 4685–4691.

Nur, A. W., Rijal, B. M. D. M., Mustafa, D. W., & Nelvi. (2024). Tanggung Jawab Pelaksana Sistem Elektronik dalam Melindungi Informasi Pemakai Media Sosial Menurut Undang-undang Nomor 19 Tahun 2016 Mengenai Informasi dan Transaksi Elektronik. *Legal Journal of Law*, *3*(1), 18–29.

Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis, Legis. No. 24 (2022).

Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Legis. No. 71 (2019).

Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce. *Jurnal Rechts Vinding Media Pembinaan Hukum Nasional*, *12*(2). https://doi.org/10.33331/rechtsvinding.v12i2.1285

Sabila, S. N., & Atman, W. (2025). Studi Kasus Kebocoran Data SIM Card oleh Bjorka: Dampaknya terhadap Kepercayaan Publik terhadap Keamanan Digital di Indonesia. *Sosial Simbiosis : Jurnal Integrasi Ilmu Sosial Dan Politik*, *2*(3), 142–154. https://doi.org/10.62383/sosial.v2i3.1998

Safira, S. D., Setyaningrum, R. P., Anwar, N. R., Aldrin, M., Noto, I. M. C. D., & Fathihah, M. A. N. (2025). Analisis Kepatuhan Etika Profesi dan Keamanan Sistem: Studi Kasus Kebocoran Data BPJS Kesehatan. *Informasi Interaktif : Jurnal Informatika Dan Teknologi Informasi*, *10*(2). https://informasiinteraktif.janabadra.ac.id/index.php/jii/article/view/157

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. https://doi.org/10.37481/jmh.v5i2.1336

Sorisa, C., Kiareni, C. L., & Parhusip, J. (2024). Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia. *JOURNAL SAINS STUDENT RESEARCH*, *2*(6), 586–593. https://doi.org/10.61722/jssr.v2i6.2996

Suyahman, S. (2025). Manajemen dan Kebijakan Keamanan Informasi. *PT Solusi Administrasi Hukum*. https://journal.sah.co.id/index.php/publisher/article/view/50

Tuzzahra, A., Aqila, D., Arenja, R. S., Naifah, S., Rinovi, N. A., & Sukma, M. (2026). Transformasi Digital Kesehatan di Indonesia: Analisis Komprehensif Peran dan Tantangan Rekam Medis Elektronik. *Jurnal Teknologi Sistem Informasi*, *7*(1), 59–68.

Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Legis. No. 1 (2024).

Undang-undang (UU) Nomor 17 Tahun 2023 tentang Kesehatan, Legis. No. 17 (2023).

Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Legis. No. 27 (2022).