Volume 11 Issue 3, 2025
P-ISSN: 2442-8019, E-ISSN: 2620-9837

PERTANGGUNGJAWABAN RUMAH SAKIT ATAS PELANGGARAN PELINDUNGAN DATA PRIBADI PASIEN PASCA UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI

Gabriella Aurel Kathleen[1], Iga Kalaringga[2], Boedi Prasetyo[3]

[1] Magister Hukum, Sekolah Tinggi Hukum Militer, Indonesia. E-mail: gabriella@gmail.com
[2] Magister Hukum, Sekolah Tinggi Hukum Militer, Indonesia.
[3] Magister Hukum, Sekolah Tinggi Hukum Militer, Indonesia.

Abstract: *Digital transformation in the health sector has accelerated the use of Electronic Medical Records (EMR) and improved healthcare efficiency; however, it has also increased the risk of personal data breaches involving patients' sensitive information. Indonesia's Personal Data Protection Law (Law No. 27/2022) establishes a comprehensive regulatory framework governing the processing of personal and health data, positioning hospitals as data controllers with strict legal responsibilities. This article aims to analyze the scope of hospitals' legal liability for patient data breaches and examine their legal status as data controllers under the Personal Data Protection Law. This study employs a normative juridical method, using statutory and conceptual approaches to assess relevant legislation, including the PDP Law, Health Law, and sectoral regulations on medical records and electronic systems. The analysis shows that hospitals can be held legally accountable in civil, administrative, and criminal domains when they fail to maintain the confidentiality and security of patient data. The findings also indicate that many hospitals face significant challenges in complying with PDP obligations, including limited cybersecurity infrastructure, inadequate human resource capacity, and low awareness of data protection principles. This paper concludes that hospitals must strengthen governance, improve technical safeguards, appoint Data Protection Officers, and enhance staff competency to ensure patient data security and meet legal compliance in the digital health era.*

Keywords: *Hospital; Patient Personal Data; Legal Responsibility; PDP Law; Privacy.*

How to Site: Gabriella Aurel Kathleen, Iga Kalaringga, Boedi Prasetyo (2025). Pertanggungjawaban Rumah Sakit Atas Pelanggaran Pelindungan Data Pribadi Pasien Pasca Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. Jurnal hukum *to-ra*, 11 (3), pp. 531-545. DOI. 10.55809/tora.v11i3.630

Introduction

Perkembangan teknologi informasi telah mendorong sektor kesehatan untuk melakukan transformasi digital dalam pelayanan medis. Rekam medis elektronik (*Electronic Medical Records*/EMR) kini digunakan luas oleh rumah sakit untuk mempercepat proses administrasi, meningkatkan efisiensi, serta memudahkan integrasi data antarinstansi. Namun, kemajuan ini juga menghadirkan tantangan serius berupa potensi pelanggaran terhadap kerahasiaan data pribadi pasien. Kasus kebocoran data

BPJS Kesehatan yang terungkap pada tahun 2021 menjadi bukti nyata lemahnya tata kelola data kesehatan di Indonesia, sehingga menimbulkan keresahan publik sekaligus menurunkan kepercayaan masyarakat terhadap institusi layanan Kesehatan.

Sebelum diundangkannya UU PDP, perlindungan data pasien hanya diatur secara parsial dalam Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan dan Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit. Kedua regulasi ini mewajibkan tenaga kesehatan dan pihak rumah sakit menjaga kerahasiaan rekam medis, namun tidak memberikan mekanisme pertanggungjawaban yang komprehensif ketika pelanggaran terjadi. Oleh sebab itu, kehadiran UU PDP menjadi tonggak penting dalam membangun kerangka hukum perlindungan data pribadi di Indonesia. UU PDP menempatkan data kesehatan pasien sebagai kategori data sensitif yang memiliki standar perlindungan lebih tinggi. Dalam konteks ini, rumah sakit berperan tidak hanya sebagai institusi pelayanan, tetapi juga sebagai pengendali data (data controller) yang wajib mematuhi prinsip-prinsip pengelolaan data pribadi. Dengan demikian, isu mengenai pertanggungjawaban rumah sakit menjadi relevan, khususnya pasca UU PDP berlaku.

Di Indonesia, walaupun sudah ada beberapa regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Kesehatan, penerapan perlindungan hukum tersebut masih menemui berbagai hambatan. Salah satu kendala utama adalah kurangnya infrastruktur keamanan teknologi yang memadai di banyak fasilitas kesehatan, di mana perlindungan siber sering kali belum optimal untuk menangkal ancaman seperti peretasan dan kebocoran data. Selain itu, kesadaran para tenaga kesehatan mengenai pentingnya menjaga kerahasiaan data pasien masih tergolong rendah, sehingga meningkatkan potensi terjadinya pelanggaran. Di sisi lain, pengawasan serta penegakan hukum terhadap pelanggaran privasi data pasien belum efektif, sehingga banyak kasus pelanggaran tidak mendapatkan penanganan yang tegas. Selain itu, ancaman dari luar berupa serangan siber yang semakin marak menjadi tantangan besar, karena data pasien kini semakin sering menjadi sasaran pihak-pihak yang tidak bertanggung jawab.

Perlindungan hukum bagi pasien saat ini semakin berkurang, suatu kondisi yang sangat disesalkan karena pasien sangat memerlukan penghormatan terhadap hak asasinya dan hak asasi manusia secara umum. Namun, ada beberapa alasan yang menyebabkan hak-hak pasien terkadang diabaikan. Menurut Satjipto Raharjo, perlindungan hukum diberikan kepada masyarakat agar mereka dapat sepenuhnya menikmati hak-hak yang diizinkan (Rahardjo, 2002). Kasus kebocoran data pribadi pasien dalam rekam medis dapat terjadi akibat faktor internal maupun eksternal. Faktor internal meliputi kurangnya tenaga sumber daya manusia yang memadai di rumah sakit, kelalaian

tenaga medis dalam menjaga kerahasiaan rekam medis pasien, serta tindakan sengaja yang dilakukan oleh beberapa pihak untuk membocorkan data pribadi pasien demi keuntungan pribadi. Selain itu, ketidakpahaman tenaga medis terhadap pentingnya menjaga kerahasiaan rekam medis, yang seharusnya hanya dapat diakses oleh pihak tertentu, juga menjadi penyebab terjadinya kebocoran. Sementara itu, faktor eksternal berasal dari kondisi di luar rumah sakit. Oleh karena itu, studi ini bertujuan untuk menganalisis bagaimana pengaturan pertanggungjawaban hukum rumah sakit terhadap kebocoran data pasien, dan bagaimana kedudukan rumah sakit sebagai pengendali data menurut UU PDP yang bertujuan untuk mencipatkan kepastian hukum.

Discussion

Pengaturan Pertanggungjawaban Hukum Rumah Sakit Atas Pembukaan Data Pribadi Pasien

Warren dan Brandeis (1890) sebagaimana dikutip oleh Sugeng pertama kali mengembangkan konsep privasi dalam sebuah artikel yang berjudul *The Right to Privacy*, yang menguraikan, "*Privacy is the right to enjoy life and the right to be left alone and this development of the law was inevitable and demanded of legal recognition*."[1] Hak privasi melalui upaya pelindungan data pada dasarnya menjadi kunci bagi kebebasan dan harga diri tiap individu. Namun, data pribadi seringkali dijadikan suatu aset dan/atau komoditi yang memiliki nilai ekonomi yang tinggi.[2] Situasi ini menimbulkan risiko bagi setiap individu karena kemungkinan terjadinya pelanggaran data pribadi selalu ada, tidak hanya dalam aktivitas yang dilakukan secara langsung (luring), tetapi juga dalam kegiatan yang berlangsung secara online (daring).

Secara filosofis, perlindungan data pribadi mencerminkan upaya menjaga hak-hak fundamental manusia yang selaras dengan nilai-nilai Pancasila. Meskipun Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945) tidak secara eksplisit mengatur pelindungan data privasi, undang-undang dasar ini tetap menjadi dasar hukum utama bagi perlindungan tersebut. Perlindungan data pribadi dipahami sebagai bagian dari hak atas privasi, di mana data yang melekat pada setiap individu dianggap sebagai hak milik yang melekat pada diri pribadi dan layak mendapatkan perlindungan. Secara tersirat, ketentuan perlindungan privasi terdapat dalam Pasal 28G ayat (1) UUD NRI yang menyatakan bahwa setiap orang berhak atas perlindungan terhadap diri sendiri, keluarga, kehormatan, martabat, dan harta benda yang dikuasainya, serta berhak merasakan rasa aman dan terlindungi dari ancaman yang menimbulkan ketakutan untuk bertindak atau tidak bertindak sesuai hak asasi. Selain

[1] Warren, S., & Brandeis, L. D. (1890). The rights to privacy. Harvard Law Review, 4.
[2] Makarim, E. (2003). Kompilasi hukum telematika. Jakarta: RajaGrafindo Perkasa.

itu, Pasal 28H ayat (4) menegaskan bahwa , "Setiap individu memiliki hak milik pribadi yang tidak boleh diambil secara sewenang-wenang oleh pihak manapun"[3] Dengan demikian, kedua pasal tersebut berfungsi sebagai dasar hukum yang menjamin perlindungan data pribadi sekaligus memberikan kepastian hukum.

Secara umum, UU PDP terdiri dari 76 Pasal dan mengatur ketentuan standar untuk pelindungan data pribadi yang wajib dijadikan acuan oleh semua sektor yang melibatkan pemrosesan data pribadi dalam penyelenggaraannya. Pengaturan dasar yang dimuat diantaranya (1) jenis data pribadi; (2) hak subjek data pribadi; (3) pemrosesan data pribadi; (4) kewajiban pengendali dan prosesor data pribadi dalam pemrosesan data pribadi; (5) transfer data pribadi; (6) sanksi administratif; (7) kelembagaan; (8) penyelesaian sengketa dan hukum acara; (9) larangan dalam penggunaan data pribadi; dan (10) ketentuan pidana. Dalam hal ini, hukum pelindungan data pribadi di Indonesia akan berlaku tidak hanya bagi orang peseorangan dan korporasi, namun juga menjangkau lembaga eksekutif, legislatif, yudikatif dan badan publik lainnya sebagaimana diatur dalam ketentuan peraturan perundang-undangan, serta organisasi yang diakui sebagai subjek hukum internasional dan mempunyai kapasitas untuk membuat perjanjian internasional.[4]

Undang-Undang Perlindungan Data Pribadi (UU PDP) mendefinisikan data pribadi sebagai informasi mengenai individu yang dapat dikenali secara langsung maupun tidak langsung, baik secara sendiri maupun melalui kombinasi dengan informasi lain, baik melalui sistem elektronik maupun non-elektronik. Berdasarkan definisi ini, sebuah data atau gabungan data hanya dapat dianggap sebagai data pribadi jika data tersebut mampu mengidentifikasi seseorang secara spesifik. Contohnya, nomor telepon seluler tanpa adanya data pendukung lainnya seperti nama lengkap, tidak termasuk data pribadi. Namun, bila nomor telepon tersebut disertai dengan nama pemilik atau alamat, maka berhasil dikategorikan sebagai data pribadi.

Perlindungan data pribadi juga diatur dalam Hukum Kesehatan, yang menegaskan bahwa data kesehatan harus dijaga kerahasiaannya. Hal ini tercantum dalam Pasal 4 Ayat (1) Huruf I Undang-Undang Nomor 117 Tahun 2023 tentang Kesehatan (UU Kes) yang menyatakan bahwa setiap individu berhak mendapatkan perlindungan atas kerahasiaan data dan informasi kesehatan pribadinya.[5] Pasal tersebut secara tegas mengatur hak setiap orang untuk menjaga kerahasiaan data dan informasi kesehatan

[3] Penjelasan Umum Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi
[4] Pasal 1 Angka 8, 9 dan 10 Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (UU PDP).
[5] Andzikriyanto Purnomo, Muhammad Mashuri, Humiati, *Akibat Hukum Bagi Rumah Sakit Terhadap Penyebarluasan Data Rekam Medis Pasien*, Jurnal Ners 4865-4874.

pribadi yang telah disampaikan kepada penyelenggara layanan kesehatan. Berdasarkan Pasal 3 ayat (2) PERMENKES Nomor 24 tahun 2022 tentang Rekam Medis,

Fasilitas pelayanan Kesehatan terdiri atas:

a) Tempat praktik mandiri dokter, dokter gigi, dan/atau Tenaga Kesehatan lainnya;
b) puskesmas;
c) Klinik;
d) Rumah Sakit;
e) Apotek;
f) Laboratorium Kesehatan;
g) Balai;
h) Fasilitas Kesehatan lain yang ditetapkan oleh Menteri.

Selain itu, Pasal 177 Ayat (1) UU Kes mewajibkan setiap Fasilitas Pelayanan Kesehatan untuk menyimpan rahasia kesehatan pasien. Selanjutnya, Pasal 274 bersama dengan Pasal 301 UU Kes menegaskan bahwa tenaga medis dan tenaga kesehatan wajib menjaga kerahasiaan kesehatan pasien dalam menjalankan praktiknya. Secara umum, data kesehatan merupakan informasi yang sangat sensitif bagi setiap individu, sehingga menjaga kerahasiaan data rekam medis menjadi tanggung jawab wajib bagi semua pihak yang terlibat dalam penyelenggaraan rekam medis elektronik. Jika kewajiban ini dilanggar, baik karena kelalaian maupun tindakan sengaja, fasilitas pelayanan kesehatan sebagai pihak yang menyelenggarakan rekam medis elektronik dapat dikenai sanksi. Namun, dalam Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis, belum dijelaskan secara rinci mengenai pertanggungjawaban atas kebocoran data rekam medis elektronik yang berasal dari sistem mitra (partner system). Perlu ditekankan bahwa dalam sistem mitra ini, fasilitas pelayanan kesehatan bekerjasama dengan penyedia sistem elektronik eksternal, sehingga perlu ada batasan yang jelas mengenai siapa yang bertanggung jawab apabila terjadi kebocoran data rekam medis elektronik. Rahasia kesehatan pasien tercatat dalam rekam medis di setiap Fasilitas Pelayanan Kesehatan, yang diatur dalam Pasal 1 Angka 1 Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis (Permenkes RM). Rekam medis merupakan dokumen yang memuat data identitas pasien, hasil pemeriksaan, pengobatan, tindakan, serta layanan lain yang telah diberikan kepada pasien. Pemanfaatan Rekam Medis Elektronik (RME) memperbaiki efisiensi dalam pengelolaan data pasien dan mengurangi kemungkinan kesalahan manusia, sehingga mendukung peningkatan mutu layanan kesehatan secara menyeluruh.[6]

[6] R. Nugraha, "Perlindungan Data Pribadi Dalam Sistem Informasi Elektronik," Bandung: Citra Aditya Bakti. (2020).

Undang-Undang PDP secara tegas menegaskan bahwa setiap pengendali data pribadi, termasuk rumah sakit, dapat dimintai pertanggungjawaban apabila terjadi pelanggaran perlindungan data pasien. Pertanggungjawaban hukum tersebut mencakup ranah perdata, administratif, dan pidana. Dalam ranah perdata, Pasal 12 UU PDP memberikan hak kepada subjek data untuk menuntut ganti rugi apabila terjadi kerugian akibat pelanggaran perlindungan data. Hal ini memberikan dasar hukum bagi pasien yang mengalami kerugian finansial maupun non-finansial akibat kelalaian rumah sakit untuk menuntut kompensasi di pengadilan. Dalam aspek administratif, Pasal 57 UU PDP memberi kewenangan kepada otoritas pelindungan data pribadi untuk menjatuhkan sanksi kepada pengendali data. Sanksi administratif yang dapat dijatuhkan meliputi teguran tertulis, penghentian sementara kegiatan pemrosesan data, penghapusan data pribadi, hingga pengenaan denda administratif. Selain itu, UU PDP juga memuat sanksi pidana. Pasal 67 UU PDP mengatur ancaman pidana penjara hingga enam tahun serta pidana denda yang tinggi bagi pihak yang secara melawan hukum mengungkapkan atau menyalahgunakan data pribadi. Jika pelanggaran dilakukan oleh korporasi, termasuk rumah sakit, maka pidana denda dijatuhkan kepada badan hukum, sementara individu yang secara langsung bertanggung jawab juga dapat dikenakan sanksi pidana.

Pembukaan data pribadi wajib mendapatkan izin pasien sesuai Pasal 26 Undang-Undang Republik Indonesia Nomor 29 Tahun 2016 tentang Perubahan Atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mengatakan penggunaan data pribadi harus dilakukan dengan persetujuan pemilik data tersebut. Hal yang sama juga diatur pada Pasal 22 UU PDP yang menyebutkan:

1. Persetujuan pemrosesan Data Pribadi dilakukan melalui persetujuan tertulis atau terekam.
2. Persetuiuan sebagaimana dimaksud pada ayat (1) dapat disampaikan secara elektronik atau nonelektronik.
3. Persetujuan sebagaimana dimaksud pada ayat (1) mempunyai kekuatan hukum yang sama.
4. Dalam hal persetujuan sebagaimana dimaksud pada ayat (1) memuat tujuan lain, permintaan persetqjuan harus memenuhi ketentuan:
    a. dapat dibedakan secara jelas dengan hal lainnya;
    b. dibuat dengan forrnat yang dapat dipahami dan mudah diakses; dan
    c. menggunalan bahasa yang sederhana dan jelas.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, atau yang dikenal dengan PP PSE[7], pada dasarnya mengatur kewajiban bagi penyelenggara sistem elektronik untuk melindungi keamanan data serta menekankan pentingnya mendapatkan persetujuan dari pemilik data sebelum data tersebut dapat digunakan oleh PSE, sebagaimana diatur dalam Pasal 14 PP PSE. Apabila dikaitkan dengan Pasal 25 ayat (2) Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis menyebutkan bahwa fasilitas pelayanan kesehatan memiliki tanggung jawab atas kehilangan, kerusakan, pemalsuan, dan/atau penyalahgunaan dokumen rekam medis oleh pihak yang tidak berwenang, baik individu maupun badan. Terkait dengan status kepemilikan ini, fasilitas pelayanan kesehatan harus menanggung konsekuensi moral dan hukum, sementara tenaga kesehatan yang terlibat dalam pelayanan juga wajib menjaga kerahasiaan informasi pasien yang tercantum dalam rekam medis tersebut.

Secara prinsip, isi rekam medis merupakan hak milik pasien, sementara berkas rekam medis dalam bentuk fisik menjadi milik rumah sakit atau institusi kesehatan. Ketentuan ini sesuai dengan Pasal 12 Peraturan Menteri Kesehatan Republik Indonesia Nomor 269 Tahun 2008 tentang Rekam Medis. Menjaga keamanan penyimpanan data dan informasi serta memudahkan akses menjadi tuntutan dari pihak ketiga yang berwenang, namun pihak yang menggunakan data atau informasi harus selalu menghormati privasi pasien. Aspek keamanan, privasi, kerahasiaan, dan keselamatan menjadi elemen penting yang melindungi data dan informasi dalam rekam kesehatan. Oleh karena itu, semua pihak berwenang yang memerlukan data atau informasi lebih mendetail sesuai dengan tugasnya wajib selalu menjaga keempat unsur tersebut di atas.

Kedudukan Rumah Sakit sebagai Pengendali Data

Sebagai pengendali data, rumah sakit memiliki kedudukan hukum yang strategis karena menentukan tujuan dan sarana pemrosesan data pasien. Status ini menimbulkan kewajiban hukum yang harus dipenuhi, antara lain prinsip legalitas, persetujuan eksplisit, dan keamanan data. Prinsip legalitas mengharuskan rumah sakit hanya memproses data pribadi pasien berdasarkan persetujuan yang sah. Persetujuan tersebut harus diberikan secara sadar, tertulis, dan spesifik terkait tujuan penggunaan data. Pengecualian hanya dimungkinkan dalam keadaan darurat medis di mana persetujuan tidak dapat diperoleh, misalnya untuk menyelamatkan nyawa pasien.

Selain itu, pasien memiliki hak-hak dasar sebagai subjek data, meliputi hak mengakses data pribadinya, memperbaiki data yang keliru, meminta penghapusan data, serta

[7] Pasal 14, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

menarik kembali persetujuan atas pemrosesan data. Rumah sakit berkewajiban menerapkan sistem perlindungan yang andal, termasuk enkripsi, autentikasi berlapis, dan audit kepatuhan secara berkala. UU PDP bahkan mewajibkan pengendali data untuk memberikan notifikasi paling lambat 72 jam setelah terjadinya insiden kebocoran data. Dengan demikian, kedudukan rumah sakit sebagai pengendali data tidak hanya sebatas penyedia layanan kesehatan, tetapi juga penjamin keamanan informasi pasien.

Lebih lanjut, arus digitalisasi di bidang kesehatan menggeser paradigma pelayanan di Indonesia. Rekam medis pasien yang dulunya manual kini beralih ke Rekam Medis Elektronik (RME), dikelola melalui SIMRS untuk pencatatan, penyimpanan, dan pemanfaatan data yang lebih efisien. Transformasi ini merupakan implementasi Permenkes No. 24 Tahun 2022 yang mewajibkan seluruh fasilitas kesehatan menerapkan RME paling lambat Desember 2023. Menurut UU Perlindungan Data Pribadi (UU PDP), rumah sakit diakui sebagai "Pengendali Data Pribadi," sehingga menjadi entitas utama yang bertanggung jawab penuh atas data sensitif pasien. Rumah sakit berwenang menentukan tujuan pengumpulan, mengendalikan pemrosesan, hingga penghapusan data. Status hukum ini menempatkan rumah sakit dalam posisi sentral perlindungan data, dengan kewajiban mematuhi regulasi ketat.

UU PDP membagi informasi pribadi menjadi Data Pribadi Umum dan Data Pribadi Spesifik. Pasal 4 ayat (2) menegaskan data kesehatan, biometrik, dan genetika termasuk kategori spesifik. Karena sensitivitasnya tinggi, rumah sakit wajib menerapkan standar keamanan siber dan fisik yang lebih ketat dibanding entitas yang hanya menangani data umum. Pelanggaran atas data spesifik dinilai serius dan berpotensi berujung sanksi berat, mendorong rumah sakit berinvestasi dalam teknologi perlindungan ekstra.

UU PDP berlandaskan standar internasional, khususnya GDPR. Prinsipnya menuntut pemrosesan data adil, transparan, dengan tujuan terbatas, data minim, akurat, dan aman. Rumah sakit wajib memastikan pasien memahami penggunaan data, meminimalisasi risiko, serta menjaga integritas informasi. Persetujuan sah pasien wajib diperoleh sebelum pemrosesan data, yang harus sukarela, spesifik, dan jelas. Pasien berhak menarik kembali persetujuan kapan saja, menuntut rumah sakit memiliki sistem yang fleksibel dan responsif. Selain itu, pasien berhak mengakses, memperbaiki, atau menghapus data, dan rumah sakit wajib menanggapi permintaan ini sesuai tenggat UU PDP.

Untuk itu, rumah sakit harus menyiapkan prosedur formal yang mencegah akses ilegal, seperti validasi KTP atau surat kuasa bermaterai. Aturan ini juga berlaku pada data pasien meninggal, menegaskan bahwa privasi di sektor kesehatan bersifat kekal. Pelanggaran UU PDP dapat berujung sanksi administratif (Pasal 57), dari teguran hingga

denda hingga 2% pendapatan tahunan. Selain itu, kebocoran data berisiko merusak reputasi rumah sakit secara permanen, yang kerugiannya sering lebih besar daripada denda.

Namun, implementasi UU PDP di sektor kesehatan masih menghadapi tantangan: lemahnya infrastruktur keamanan, rendahnya literasi privasi, serta pengawasan yang belum optimal, membuat risiko kebocoran tetap tinggi. Sebagai kesimpulan, posisi rumah sakit sebagai pengendali data menuntut tanggung jawab hukum dan moral besar. Hanya dengan kebijakan ketat, SDM mumpuni, infrastruktur IT yang kuat, dan kepatuhan regulasi, rumah sakit dapat meminimalkan risiko hukum sekaligus membangun kepercayaan publik di era digital.

Pengaturan Hukum Positif Indonesia Mengatur Perlindungan Data Pribadi Pasien di Rumah Sakit

Perubahan digital di sektor kesehatan mempermudah akses data pasien dan mendorong telemedicine, namun memunculkan masalah perlindungan data pribadi. Secara hukum, aturan sudah ada, tetapi implementasinya belum optimal karena kendala teknis, regulasi, SDM, dan ancaman eksternal (Yusuf, 2022).Data pribadi dalam rekam medis adalah informasi sensitif yang menyangkut harkat martabat pasien, meliputi identitas, riwayat medis, hingga hasil pemeriksaan. Informasi ini wajib dijaga kerahasiaannya sebagai bagian dari *privacy right* yang dilindungi konstitusi dan peraturan perundang-undangan. Hukum positif Indonesia, melalui UU No. 27 Tahun 2022, UU No. 36 Tahun 2009, dan Permenkes No. 24 Tahun 2022, mewajibkan rumah sakit menjaga kerahasiaan data pasien. Pelanggaran terhadap kewajiban ini, seperti penyebarluasan rekam medis tanpa izin, dapat dikenai sanksi hukum untuk memberikan hukuman, menciptakan keseimbangan hak dan kewajiban, serta menjaga kepercayaan pasien.

Pasal 34 UU PDP mengizinkan rumah sakit memproses data spesifik seperti rekam medis, dengan syarat utama melakukan Penilaian Dampak Pelindungan Data Pribadi (*Data Protection Impact Assessment*) untuk mencegah risiko yang merugikan pasien. Selanjutnya, Pasal 36 UU PDP mewajibkan pengendali data menjaga kerahasiaan data pasien. Pelanggaran atas kewajiban ini dapat dikenai sanksi administratif berlapis, mulai dari peringatan tertulis, penghentian sementara pemrosesan data, penghapusan data, hingga denda administratif.

Pasal 65 UU PDP merinci larangan penggunaan data pribadi yang menjadi dasar sanksi pidana. Jika rumah sakit menyebarkan rekam medis tanpa dasar hukum, konsekuensinya adalah pertanggungjawaban pidana. Perlindungan ini diperjelas dalam Pasal 67 UU PDP, yang mengatur sanksi pidana bagi pelanggar prinsip pengelolaan data.

Pasal 70 UU PDP menekankan sanksi pidana jika pelanggaran dilakukan oleh korporasi seperti rumah sakit. Menurut Pasal 70 ayat (1), sanksi dapat dijatuhkan kepada korporasi beserta pengurus atau pihak yang bertanggung jawab. Pasal 70 ayat (2) UU PDP menyatakan korporasi hanya dapat dijatuhi pidana denda, namun dimungkinkan adanya pidana tambahan seperti perampasan keuntungan, pembekuan kegiatan, pencabutan izin, hingga perintah membayar ganti rugi kepada pasien. Ketentuan ini menempatkan rumah sakit pada posisi strategis sebagai Pengendali Data Pribadi yang harus siap menghadapi konsekuensi hukum berat jika terjadi pelanggaran, sebagai jaminan negara atas hak privasi pasien.

Dalam teori Satjipto Rahardjo, terdapat dua bentuk perlindungan hukum: preventif dan represif. Perlindungan preventif berupaya mencegah pelanggaran melalui regulasi dan SOP. Sementara itu, perlindungan represif diterapkan setelah pelanggaran terjadi untuk menyelesaikan konflik, memulihkan hak, dan memberi efek jera. Pelindungan hukum represif diwujudkan melalui sanksi pidana, perdata, dan administratif. Sanksi pidana berupa penjara atau denda untuk pelanggaran serius. Sanksi perdata dapat ditempuh melalui gugatan ganti rugi berdasarkan Pasal 1365 KUHPerdata. Sanksi administratif dijatuhkan kepada penyelenggara yang lalai menjaga keamanan data. Sanksi administratif diatur dalam Pasal 100 ayat (1) dan (2) PP No. 71 Tahun 2019, yang mencakup teguran tertulis, denda, penghentian sementara, hingga pencabutan dari daftar penyelenggara. Instrumen ini menegaskan kehadiran negara dalam memastikan data pasien tidak disalahgunakan.[8]

Dengan demikian, perlindungan hukum represif atas data pribadi pasien bertujuan menciptakan keadilan (menjamin hak privasi pasien), kemanfaatan (pemanfaatan data untuk publik secara sah), dan kepastian hukum (regulasi dan sanksi yang jelas). Kombinasi perlindungan preventif dan represif menjadi pilar utama untuk menjaga kepercayaan pasien dan memperkuat implementasi hukum. Namun, masih ada perdebatan mengenai informasi apa yang harus disampaikan kepada pasien terkait kepemilikan rekam medis. Oleh karena itu, resume medis dibuat sebagai kompromi

untuk memenuhi hak pasien sambil menjaga ketertiban[9], di mana berkas rekam medis tidak boleh dibawa oleh pasien dan menjadi tanggung jawab rumah sakit.[10] Salah satu

[8] *Peraturan Pemerintah* Republik Indonesia *Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*, Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185

[9] Arief Dilan Santoso, Aldi Sulistiyono, dan Isharyanto. 2019. *"Majelis Kehormatan Disiplin Kedokteran Indonesia (MKDKI) untuk Dapat Menjamin Keadilan dalam Hubungan Dokter dan Pasien."* Jurnal Pascasarjana Hukum UNS, Vol. 21, No. 1, hlm. 29–38

[10] Rian Saputra dan Resti Dian Luthviati. 2020. *"Institutionalization of the Approval Principle of Majority Creditors for Bankruptcy Decisions in Bankruptcy Act Reform Efforts."* Journal of Morality and Legal Culture (JMCL), Vol. 3, No. 2, hlm. 112–114

hambatan utama adalah keterbatasan infrastruktur TI. Banyak rumah sakit belum memiliki fasilitas memadai, seperti SIMRS yang tidak terenkripsi atau sistem cadangan data dan perlindungan siber yang cukup, seperti *firewall* atau antivirus (Nurhayati, 2022).

Secara filosofis, substansi pengaturan lebih menekankan perlindungan hak privasi pasien, sementara aspek perlindungan isi rekam medis belum seimbang.[11] Meskipun rekam medis milik pasien, ketentuan kepentingan umum terkait hal ini belum jelas dalam hukum positif. Pengaturan hanya ada di Pasal 57 UU Kesehatan, yang menyatakan hak atas rahasia kondisi kesehatan tidak berlaku dalam hal:

1. Perintah undang-undang;
2. Perintah pengadilan;
3. Izin dari pihak yang bersangkutan;
4. Kepentingan masyarakat; atau
5. Kepentingan orang tersebut.

Sebagaimana dijabarkan, kebocoran data rekam medis sering dikaitkan dengan poin ke-4 mengenai kepentingan masyarakat. Namun, frasa "kepentingan masyarakat" ini masih terkesan abstrak karena belum ada peraturan turunan yang mendefinisikan secara jelas konteks dan indikatornya.[12]Layanan E-Health mengumpulkan data pribadi sensitif, sehingga menimbulkan masalah hukum terkait kewajiban penyelenggara melindungi data tersebut dari akses tidak sah. Jika data pribadi digunakan tanpa izin, hal itu melanggar hak dasar atas privasi yang dijamin oleh hukum internasional dan nasional. Berdasarkan konsep kepemilikan, rekam medis milik pasien seharusnya berfungsi sosial untuk manfaat luas bagi masyarakat. Namun, manfaat tersebut tidak menghapus hak pasien, sehingga persetujuan atau kompensasi tertentu tetap diperlukan saat rekam medisnya digunakan untuk kepentingan umum. Keterlibatan masyarakat dalam pemberdayaan fungsi sosial rekam medis memerlukan peran negara melalui hukum positif. Rekam medis harus tetap dipandang sebagai hak milik pasien. Artinya, pengalihannya tidak dapat dilakukan secara bebas seperti hak milik atas benda pada umumnya, karena menyangkut hak atas kehormatan pasien yang absolut. Dengan demikian, fungsi sosial rekam medis harus dijalankan dengan menghormati hak pasien.

Rekam medis digunakan untuk berbagai kepentingan, seperti alat bukti hukum, administrasi, pendidikan, penelitian, dan statistik kesehatan. Pemanfaatan oleh pemerintah tidak memerlukan persetujuan langsung selama hak privasi pasien

[11] Sonya Alrini Batubara. 2020. "Kekuatan Hukum Pembuktian Rekam Medis Konvensional dan Elektronik Berdasarkan Hukum Positif Indonesia." Jurnal Hukum Samudra Keadilan, Vol. 2, No. 1, hlm. 73–75.
[12] Guwandil, J., *Hukum Medik*, Jakarta: Fakultas Kedokteran Universitas Indonesia, 2018, hlm. 181.

dihormati. Namun, jika digunakan pihak lain, persetujuan pasien wajib diperoleh. Penggunaan tanpa persetujuan sah dapat dianggap pelanggaran hukum. Menurut Pasal 1365 KUHPerdata, "Tiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang karena salahnya menerbitkan kerugian itu, mengganti kerugian tersebut."[13] Penggunaan rekam medis tanpa izin memenuhi unsur perbuatan melawan hukum (PMH). Jika timbul kerugian, baik materiil maupun immateriil, pasien dapat mengajukan gugatan ganti rugi.

Meskipun rekam medis milik pasien, pemanfaatannya untuk kepentingan umum belum diatur jelas. UU Praktik Kedokteran, UU Kesehatan, dan UU PDP mengklasifikasikan data kesehatan sebagai data sensitif yang harus dilindungi, namun belum memberikan batasan konkret bagaimana kepentingan umum dapat mengesampingkan hak pasien. Akibatnya, muncul celah interpretasi dan ketidakpastian hukum, yang berpotensi menimbulkan konflik antara hak privasi pasien dan kebutuhan publik. Diperlukan peraturan turunan yang lebih komprehensif untuk memberikan kepastian hukum dan menjaga keseimbangan antara kepentingan individual dan masyarakat.

Kementerian Kesehatan melaporkan bahwa baru sekitar 40% rumah sakit yang memiliki SIMRS dengan sistem terintegrasi dan aman, yang mencerminkan rendahnya kesiapan teknologi dalam memenuhi amanat Permenkes No. 24 Tahun 2022 serta UU PDP.

1. **Keterbatasan Infrastruktur Teknologi Informasi** Sebagian besar rumah sakit, terutama di daerah, masih memiliki infrastruktur TI terbatas. SIMRS yang tidak terstandarisasi dan tidak terenkripsi menyebabkan potensi kebocoran data yang tinggi. Banyak rumah sakit juga belum memiliki sistem cadangan atau keamanan siber yang memadai (Nurhayati, 2025). Menurut Kementerian Kesehatan, hanya sekitar 40% rumah sakit yang memiliki SIMRS terintegrasi dan aman, menunjukkan lemahnya kesiapan teknologi untuk mendukung regulasi seperti Permenkes No. 24 Tahun 2022 dan UU PDP.

2. **Rendahnya Pemahaman dan Kesadaran SDM** Tenaga kesehatan dan manajemen rumah sakit sering kali belum memahami regulasi perlindungan data pribadi. Kesadaran akan pentingnya kerahasiaan data belum merata, sehingga praktik tidak aman seperti pengaksesan tanpa izin atau pengiriman data melalui media tidak aman masih terjadi (Amalia, 2022). Kelemahan ini mengakibatkan potensi pelanggaran hukum, baik disengaja maupun karena kelalaian.

[13] Kitab Undang-Undang Hukum Perdata (Burgerlijk Wetboek voor Indonesie).

3. **Ancaman Serangan Siber** Serangan siber terhadap layanan kesehatan meningkat pesat. Data Kementerian Komunikasi dan Informatika menunjukkan sektor kesehatan menjadi target utama peretasan data pada 2022–2023. Rumah sakit rentan karena data yang dimilikinya bernilai tinggi. Serangan seperti *ransomware* dan *phishing* tidak hanya merugikan institusi tetapi juga berdampak langsung pada hak privasi pasien.

4. **Ketidaksinkronan Regulasi** Tantangan lainnya adalah tumpang tindih regulasi sektoral seperti Permenkes No. 24/2022 dengan UU PDP. Beberapa ketentuan teknis belum diperbarui untuk menyesuaikan dengan prinsip UU PDP, seperti pengangkatan *Data Protection Officer* (DPO) dan kewajiban *privacy impact assessment*. Selain itu, tidak semua rumah sakit memahami sanksi jika terjadi pelanggaran, sehingga melemahkan urgensi pembentukan struktur perlindungan data yang kuat.

Secara kumulatif, berbagai tantangan tersebut menunjukkan adanya kesenjangan signifikan antara kewajiban hukum yang diamanatkan regulasi dan kapabilitas riil di lapangan. Kegagalan dalam mengatasi keterbatasan infrastruktur, sumber daya manusia, dan keamanan siber tidak hanya menciptakan risiko hukum bagi rumah sakit sebagai pengendali data, tetapi juga mengancam hak fundamental pasien atas privasi. Oleh karena itu, diperlukan sebuah pendekatan tata kelola data yang holistik dan terintegrasi, yang tidak hanya berfokus pada pemenuhan aspek teknis tetapi juga membangun budaya sadar privasi di seluruh lapisan organisasi rumah sakit.

Conclusion

Berdasarkan analisis, Undang-Undang No. 27 Tahun 2022 (UU PDP) menetapkan rumah sakit sebagai Pengendali Data yang memiliki pertanggungjawaban hukum ketat untuk menjamin kerahasiaan dan keamanan data pribadi pasien, dengan ancaman sanksi administratif, pidana, dan perdata atas pelanggaran. Untuk memenuhi kewajiban ini, rumah sakit disarankan agar segera meningkatkan kapasitas SDM melalui pelatihan berkelanjutan, menunjuk Petugas Perlindungan Data (DPO), serta mengimplementasikan kebijakan tata kelola data yang kuat, termasuk prosedur responsif untuk memenuhi hak-hak pasien. Selain itu, investasi dalam keamanan teknis seperti audit rutin, enkripsi data, dan kontrol akses yang ketat menjadi krusial untuk memitigasi risiko hukum. Pendekatan proaktif yang mengintegrasikan kepatuhan berkelanjutan ini tidak hanya untuk menghindari sanksi, tetapi juga esensial untuk membangun dan mempertahankan kepercayaan publik yang menjadi aset fundamental dalam pelayanan kesehatan.

References

Amalia, K. F., et al. (2022). Scoping review: Hambatan penerapan telemedicine di Indonesia. Conference Series: Medical Science, 2(1), 637.

Makarim, E. (2003). Kompilasi hukum telematika. RajaGrafindo Perkasa.

Nurhayati, R. H. (2025). Legal protection for patients in telemedicine services in Indonesia. Journal of Legal, Public and Humanity, 5(3). https://doi.org/10.38035/jlph.v5i3.1592

Palito, J., et al. (2021). Urgensi pembentukan pengaturan perlindungan data pribadi di Indonesia serta komparasi pengaturan di Jepang dan Korea Selatan. Supremasi Hukum, 17(1), 23–33.

Rahardjo, S. (2002). Ilmu hukum. PT Citra Aditya Bakti.

Rosadi, S. D. (2023). Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022). Sinar Grafika.

Sugeng. (2020). Hukum telematika Indonesia (Edisi pertama). Kencana.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. (1945).

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. (2022).

Warren, S., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220.

Yusuf, R. (2022). Strategi nasional keamanan siber Indonesia: Tantangan dan solusi. Jurnal Keamanan Nasional, 30–44.