

**IMPLEMENTASI DAN TANTANGAN REGULASI PERLINDUNGAN  
DATA PRIBADI PASIEN DI ERA DIGITAL PADA RUMAH SAKIT  
*IMPLEMENTATION AND CHALLENGES OF PATIENT PERSONAL  
DATA PROTECTION REGULATION IN THE DIGITAL ERA IN  
HOSPITALS***

**Yudha Aditya Pradana dan Wilma Silalahi**

**Fakultas Hukum Universitas Tarumanagara**

Korespondensi Penulis : [yudhalawyer28@gmail.com](mailto:yudhalawyer28@gmail.com)

Citation Structure Recommendation :

Pradana, Yudha Aditya dan Wilma Silalahi. *Implementasi dan Tantangan Regulasi Perlindungan Data Pribadi Pasien di Era Digital pada Rumah Sakit*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.5. No.12 (2024).

**ABSTRAK**

Perkembangan teknologi informasi dalam sektor kesehatan memicu kebutuhan akan sistem perlindungan data pribadi pasien yang kuat dan terpadu. Di tengah transformasi digital rumah sakit, kerentanan terhadap kebocoran data semakin tinggi. Permasalahan yang dihadapi adalah bagaimana ketentuan hukum positif di Indonesia mengatur perlindungan data pribadi pasien di rumah sakit dalam konteks transformasi digital dan apa saja tantangan yang dihadapi rumah sakit dalam mengimplementasikan regulasi perlindungan data pribadi pasien, dan bagaimana upaya yang dapat dilakukan untuk mengatasinya di era digital. Metode penelitian yang digunakan adalah penelitian hukum yuridis normatif. Hasil penelitian menunjukkan bahwa ketentuan hukum positif di Indonesia yang mengatur perlindungan data pribadi pasien meliputi UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mengklasifikasikan data kesehatan sebagai data sensitif, UU No. 36 Tahun 2009 tentang Kesehatan yang menjamin kerahasiaan informasi medis, serta Permenkes No. 24 Tahun 2022 tentang Rekam Medis yang mewajibkan rumah sakit menjaga keamanan data, baik manual maupun digital. Ketentuan ini menjadi dasar hukum dalam era transformasi digital pelayanan kesehatan. Tantangan utama rumah sakit yaitu minimnya infrastruktur, rendahnya pemahaman SDM, ancaman siber, dan tumpang tindih regulasi. Upaya solusinya: peningkatan teknologi, pelatihan SDM, penunjukan Data Protection Officer (DPO), dan penyusunan Standard Operation Procedure (SOP) serta audit rutin.

**Kata Kunci: Perlindungan Data Pribadi, Pasien di Rumah Sakit, Implementasi Regulasi, Era Digital**

**ABSTRACT**

*The development of information technology in the health sector has triggered the need for a strong and integrated patient personal data protection system. In the midst of the digital transformation of hospitals, the vulnerability to data leaks is increasing. The problem faced is how positive legal provisions in Indonesia regulate the protection of patient personal data in hospitals in the context of digital transformation and what challenges hospitals face in implementing regulations on patient personal data protection, and what efforts can be made to overcome them in the digital era. The research method used is normative juridical legal research. The results of the study show that positive legal provisions in Indonesia that regulate the protection of patient personal data include Law No. 27 of 2022 concerning Personal Data Protection which classifies health data as sensitive data, Law No. 36 of 2009 concerning Health which guarantees the confidentiality of medical information, and Permenkes No. 24 of 2022 concerning Medical Records which requires hospitals to maintain data security, both manual and digital. These provisions are the legal basis in the era of digital transformation of health services. The main challenges for hospitals are minimal infrastructure, low understanding of human resources, cyber threats, and overlapping regulations. Solution efforts: technology improvement, HR training, appointment of DPO, and preparation of SOPs and routine audits.*

**Keywords:** *Personal Data Protection, Hospital Patients, Regulation Implementation, Digital Era*

**A. PENDAHULUAN**

Perkembangan teknologi informasi yang pesat telah membawa transformasi besar dalam sistem pelayanan kesehatan, khususnya dalam pengelolaan data dan informasi pasien. Rumah sakit kini tidak hanya menjadi pusat layanan medis, tetapi juga berfungsi sebagai institusi pengelola data pribadi yang sangat sensitif, termasuk data kesehatan, rekam medis, riwayat penyakit, dan informasi demografis pasien. Transformasi digital dalam bentuk penerapan rekam medis elektronik (*Electronic Medical Records/EMR*), layanan kesehatan jarak jauh (*telemedicine*), hingga integrasi data antar fasilitas kesehatan membuat perlindungan terhadap data pribadi pasien menjadi isu yang semakin krusial. (Indriyani, 2022)

Data pribadi pasien dikategorikan sebagai *data pribadi sensitif* yang memiliki tingkat kerahasiaan tinggi. Kebocoran atau penyalahgunaan data ini dapat menimbulkan dampak serius, baik bagi pasien secara individu maupun bagi reputasi institusi kesehatan. Tidak sedikit kasus kebocoran data kesehatan yang mencuat di ruang publik dan menimbulkan keresahan masyarakat, termasuk dugaan kebocoran data dari sistem kesehatan nasional dan rumah sakit swasta.

Oleh karena itu, urgensi perlindungan data pribadi dalam sistem pelayanan kesehatan tidak hanya menyangkut aspek teknis, tetapi juga menyangkut aspek etika, hukum, dan tata kelola kelembagaan. (Kompas.com, 2025)

Di Indonesia, kerangka hukum untuk melindungi data pribadi pasien telah diatur melalui berbagai regulasi, baik bersifat umum maupun sektoral. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan instrumen hukum utama yang secara eksplisit mengklasifikasikan data kesehatan sebagai bagian dari data pribadi sensitif yang wajib mendapat perlindungan khusus. Selain itu, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan juga memberikan jaminan terhadap hak pasien atas kerahasiaan informasi medisnya. Ketentuan ini dipertegas dalam Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis yang mewajibkan rumah sakit menjaga keamanan rekam medis, baik dalam bentuk manual maupun elektronik.

Meski regulasi telah tersedia, implementasinya di tingkat rumah sakit menghadapi tantangan yang signifikan. Banyak rumah sakit, terutama di daerah, masih menghadapi keterbatasan dalam hal infrastruktur teknologi informasi yang memadai, keamanan siber yang lemah, serta minimnya pemahaman tenaga kesehatan terhadap pentingnya privasi data. Selain itu, belum sinkronnya regulasi sektoral dan lemahnya mekanisme pengawasan turut menjadi penghambat dalam pelaksanaan perlindungan data pribadi pasien secara efektif. (Agustina, 2022)

Kondisi ini diperburuk dengan meningkatnya serangan siber yang menargetkan sistem informasi kesehatan. Data dari *Indonesia Cyber Security Forum* menunjukkan bahwa rumah sakit menjadi salah satu sektor yang paling rentan terhadap serangan digital, karena nilai strategis dari data kesehatan yang dapat diperdagangkan di pasar gelap.<sup>8</sup> Maka dari itu, tantangan dalam mengimplementasikan regulasi perlindungan data pribadi tidak hanya bersifat normatif, tetapi juga operasional dan strategis. Dalam konteks ini, sangat penting untuk mengevaluasi sejauh mana regulasi yang ada dapat diimplementasikan secara efektif di lapangan, serta mengidentifikasi strategi yang dapat dilakukan untuk memperkuat perlindungan data pasien di rumah sakit. Oleh karena itu, tulisan ini bertujuan untuk mengkaji ketentuan hukum positif yang berlaku dan menganalisis tantangan serta solusi implementatif di era digital saat ini.

## **B. PEMBAHASAN**

### **Ketentuan Hukum Positif di Indonesia Mengatur Perlindungan Data Pribadi Pasien di Rumah Sakit dalam Konteks Transformasi Digital**

Transformasi digital telah mengubah wajah pelayanan kesehatan secara fundamental. Di Indonesia, digitalisasi di sektor kesehatan semakin berkembang melalui implementasi rekam medis elektronik (*electronic medical record/EMR*), sistem informasi manajemen rumah sakit (SIMRS), dan layanan *telemedicine* yang memudahkan akses layanan medis tanpa harus hadir secara fisik. Namun, transformasi ini juga membawa tantangan besar dalam aspek perlindungan data pribadi pasien. Mengingat bahwa data pasien, khususnya data medis, tergolong sebagai informasi yang bersifat sangat sensitif, maka perlindungan terhadap data itu tidak hanya menjadi tanggung jawab etis, tetapi kewajiban hukum yang diatur secara tegas dalam ketentuan hukum positif di Indonesia. (Darmawan, 2022)

Dalam konteks hukum, data pribadi adalah setiap data tentang seseorang yang dapat diidentifikasi secara langsung maupun tidak langsung. Menurut Pasal 1 angka 1 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), data pribadi mencakup informasi identitas diri seperti nama, nomor induk kependudukan, alamat, dan informasi kesehatan. UU PDP lebih lanjut mengklasifikasikan data kesehatan sebagai "data pribadi sensitif" yang membutuhkan perlakuan perlindungan yang lebih ketat dibandingkan data biasa. Perlakuan khusus ini sejalan dengan standar internasional, seperti General Data Protection Regulation (GDPR) Uni Eropa yang juga menggolongkan data kesehatan dalam kategori khusus yang memerlukan dasar hukum yang kuat untuk pengolahan.

Penting untuk dicatat bahwa pengelolaan data pribadi sensitif, seperti informasi medis, menuntut kehati-hatian tinggi karena konsekuensi hukum dan sosial dari kebocoran data sangat besar. Data pasien yang bocor bisa disalahgunakan untuk diskriminasi, pemerasan, atau bahkan pencurian identitas. Oleh sebab itu, perlindungan hukum terhadap data pribadi pasien di rumah sakit menjadi kebutuhan mendesak, khususnya dalam konteks integrasi sistem informasi dan transformasi digital pelayanan kesehatan.

Terdapat beberapa ketentuan hukum positif di Indonesia yang menjadi dasar perlindungan data pribadi pasien, baik dalam bentuk undang-undang maupun peraturan teknis sektoral, diantaranya:

1. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)

UU PDP merupakan payung hukum utama yang secara eksplisit mengatur hak dan kewajiban subjek data dan pengendali data (dalam hal ini rumah sakit atau penyelenggara sistem elektronik bidang kesehatan). Pasal 4 ayat (2) huruf b UU PDP menegaskan bahwa data kesehatan termasuk dalam kategori data pribadi sensitif. Selanjutnya, Pasal 20 UU PDP menyatakan bahwa pengendali data wajib melindungi data pribadi dari akses tidak sah, pengungkapan, perubahan, dan/atau penghapusan yang tidak sah.

UU PDP juga mengatur hak pasien sebagai subjek data, seperti hak untuk mengetahui tujuan dan dasar pemrosesan data, hak untuk menarik persetujuan, serta hak untuk mengajukan gugatan atas pelanggaran data. Dalam konteks rumah sakit, ini berarti bahwa pasien berhak mengetahui bagaimana data mereka digunakan, siapa saja yang memiliki akses, dan sejauh mana perlindungan data tersebut dijamin oleh rumah sakit sebagai pengendali data.

2. Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan

Sebelum hadirnya UU PDP, UU Kesehatan telah lebih dahulu mengatur mengenai kewajiban menjaga kerahasiaan data medis. Pasal 57 ayat (1) UU No. 36 Tahun 2009 menyatakan bahwa setiap orang berhak atas kerahasiaan kondisi kesehatan pribadinya. Pasal 57 ayat (2) lebih lanjut menyebutkan bahwa informasi tentang kesehatan hanya dapat dibuka untuk kepentingan pasien, atas permintaan penegak hukum, atau demi kepentingan masyarakat luas berdasarkan ketentuan perundang-undangan.

Ketentuan ini menjadi landasan awal bagi setiap tenaga medis, manajemen rumah sakit, dan instansi pelayanan kesehatan untuk menjaga kerahasiaan data medis pasien, sekaligus menunjukkan bahwa aspek perlindungan data pasien bukan hal yang baru, tetapi sudah menjadi kewajiban hukum yang melekat dalam pelayanan kesehatan.

### 3. Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis

Regulasi teknis yang spesifik mengatur perlindungan data pasien di rumah sakit dituangkan dalam Peraturan Menteri Kesehatan (Permenkes) No. 24 Tahun 2022 tentang Rekam Medis. Permenkes ini mengatur bahwa setiap fasilitas pelayanan kesehatan wajib menyelenggarakan dan mengelola rekam medis secara aman, terintegrasi, dan rahasia, baik dalam bentuk tertulis maupun elektronik.

Pasal 21 hingga Pasal 23 Permenkes ini menjelaskan secara rinci mekanisme pengamanan rekam medis digital, termasuk pengelolaan akses, pencatatan log akses, dan keharusan menyimpan data secara terenkripsi serta penggunaan sistem informasi yang sesuai standar keamanan. Hal ini menegaskan bahwa perlindungan terhadap data pribadi pasien tidak hanya bersifat normatif, tetapi juga teknis operasional.

Meskipun secara normatif telah tersedia berbagai instrumen hukum, tantangan yang tidak kalah penting adalah bagaimana mengharmonisasikan regulasi sektoral yang seringkali berjalan sendiri-sendiri. UU PDP sebagai regulasi umum harus disinergikan dengan UU Kesehatan dan Permenkes yang bersifat sektoral agar tidak terjadi tumpang tindih dalam penerapan. Misalnya, ketentuan tentang hak subjek data dalam UU PDP harus dikaitkan dengan prinsip kerahasiaan medis dalam UU Kesehatan, sehingga penyedia layanan kesehatan dapat menjalankan kewajibannya secara proporsional dan tidak melanggar hak konstitusional pasien. (Agustina, Sinkronisasi Regulasi Perlindungan Data di Sektor Kesehatan, 2023) Sinkronisasi regulasi juga penting dalam menyusun standar operasional prosedur (SOP) perlindungan data pribadi pasien di setiap rumah sakit, agar tidak terjadi inkonsistensi dalam implementasi. Oleh karena itu, dibutuhkan regulasi turunan yang lebih teknis dari UU PDP, khususnya di sektor kesehatan, agar pelaksanaannya lebih jelas dan terukur.

Di samping ketentuan hukum tertulis, perlindungan data pasien juga diperkuat oleh kode etik profesi kedokteran dan keperawatan. Dalam Kode Etik Kedokteran Indonesia, disebutkan bahwa setiap dokter wajib menjaga kerahasiaan segala sesuatu yang diketahuinya tentang pasien, bahkan setelah pasien meninggal dunia. Hal ini menegaskan bahwa perlindungan data bukan hanya kewajiban hukum administratif, akan tetapi juga tanggung jawab moral dan juga profesional.

Oleh karena itu, penerapan hukum positif harus berjalan seiring dengan internalisasi nilai-nilai etik dalam dunia kesehatan.

Dengan adanya berbagai instrumen hukum tersebut, dapat disimpulkan bahwa Indonesia telah memiliki kerangka hukum yang cukup komprehensif dalam melindungi data pribadi pasien, khususnya di era digital. Namun, tantangan implementasi dan harmonisasi regulasi masih menjadi pekerjaan rumah utama. Perlindungan data pribadi pasien tidak cukup hanya dengan aturan, tetapi harus diikuti dengan penguatan kelembagaan, peningkatan kesadaran hukum, dan dukungan teknologi informasi yang memadai di setiap rumah sakit.

### **Tantangan yang Dihadapi Rumah Sakit dalam Mengimplementasikan Regulasi Perlindungan Data Pribadi Pasien, dan Upaya yang Dapat Dilakukan untuk Mengatasinya di Era Digital**

Transformasi digital di sektor kesehatan telah membawa manfaat signifikan, seperti kemudahan akses data pasien, efisiensi pelayanan, hingga pengembangan layanan *telemedicine*. Namun, kemajuan ini juga melahirkan tantangan besar dalam hal perlindungan data pribadi pasien yang dikelola oleh rumah sakit. Meski secara normatif regulasi telah tersedia, realitas di lapangan menunjukkan bahwa pelaksanaan perlindungan data belum sepenuhnya efektif. Hal ini disebabkan oleh berbagai faktor teknis, regulatif, sumber daya manusia, serta ancaman eksternal yang semakin kompleks di era digital. (Yusuf, 2023) Tantangan yang dihadapi:

#### **1. Keterbatasan Infrastruktur Teknologi Informasi**

Sebagian besar rumah sakit, terutama di daerah, masih menghadapi keterbatasan infrastruktur teknologi informasi (TI). Penggunaan sistem informasi manajemen rumah sakit (SIMRS) yang tidak terstandarisasi dan tidak terenkripsi menyebabkan potensi kebocoran data tinggi. Bahkan, banyak rumah sakit belum memiliki sistem cadangan (backup) data atau sistem keamanan siber seperti *firewall*, *antivirus*, serta mekanisme deteksi intrusi. (Nurhayati, 2022)

Menurut laporan Kementerian Kesehatan, hanya sekitar 40% rumah sakit yang memiliki SIMRS terintegrasi dan aman secara digital. Hal ini menunjukkan masih lemahnya kesiapan teknologi untuk mendukung amanat regulasi, seperti yang tercantum dalam Permenkes No. 24 Tahun 2022 dan UU PDP yang mensyaratkan keamanan data pasien secara elektronik.

## 2. Rendahnya Pemahaman dan Kesadaran SDM

Tenaga kesehatan, administrator, dan manajemen rumah sakit sering kali belum memahami secara mendalam tentang regulasi perlindungan data pribadi dan etika privasi pasien. Kesadaran akan pentingnya menjaga kerahasiaan data pasien belum merata, sehingga praktik seperti pengaksesan data tanpa izin, pengiriman data melalui media tidak aman (misalnya aplikasi pesan instan), atau penyimpanan data di perangkat pribadi masih banyak terjadi. (Amelia, 2022)

Kelemahan ini mengakibatkan potensi pelanggaran hukum, baik yang disengaja maupun karena kelalaian. Padahal, menurut UU PDP, pengendali data wajib menjamin hanya pihak berwenang yang dapat mengakses dan mengolah data pribadi pasien.

## 3. Ancaman Serangan Siber

Serangan siber terhadap institusi layanan kesehatan meningkat pesat secara global dan nasional. Data Kementerian Komunikasi dan Informatika menunjukkan bahwa sektor kesehatan merupakan salah satu target utama peretasan data pada tahun 2022–2023. Rumah sakit sebagai institusi penyedia layanan publik sangat rentan karena data yang dimilikinya sangat bernilai tinggi (misalnya riwayat medis, informasi identitas, dan keuangan pasien).

Serangan seperti *ransomware*, *phishing*, dan *data breach* bukan hanya merugikan institusi dari segi reputasi dan finansial, tetapi juga berdampak langsung pada hak pasien atas privasi dan kerahasiaan informasi.

## 4. Ketidaksinkronan Regulasi

Tantangan lainnya adalah adanya tumpang tindih dan ketidaksinkronan antara regulasi teknis sektoral seperti Permenkes No. 24/2022, UU Kesehatan, dan UU PDP. Beberapa ketentuan teknis belum diperbarui untuk menyesuaikan dengan prinsip-prinsip yang diatur dalam UU PDP, seperti pengangkatan Data Protection Officer (DPO), kewajiban *privacy impact assessment*, dan pelaporan insiden pelanggaran data. (Hardiansyah, 2023)

Selain itu, tidak semua rumah sakit mengetahui atau memahami ketentuan sanksi administratif dan pidana jika terjadi pelanggaran. Hal ini mengakibatkan lemahnya urgensi dalam membentuk struktur perlindungan data yang kuat dan berkelanjutan.

Untuk menjawab berbagai tantangan di atas, diperlukan langkah-langkah konkret yang bersifat sistemik, kolaboratif, dan progresif. Upaya tersebut antara lain: (Mulyadi, 2023)

#### 1. Penguatan Infrastruktur dan Keamanan Siber

Pemerintah dan rumah sakit perlu berinvestasi dalam peningkatan teknologi informasi, baik berupa perangkat keras (hardware), perangkat lunak (software), maupun sumber daya TI. Sistem rekam medis elektronik harus menggunakan enkripsi data, sistem autentikasi ganda, dan penyimpanan berbasis server yang aman. Selain itu, rumah sakit perlu membangun sistem pemulihan bencana digital dan melibatkan tenaga ahli keamanan siber untuk melakukan audit sistem secara berkala. Penguatan infrastruktur ini sejalan dengan amanat Pasal 39 UU PDP yang mewajibkan pengendali data untuk melakukan pengamanan data pribadi dengan menerapkan prinsip *privacy by design* dan *security by default*.

Penguatan infrastruktur dan keamanan siber menjadi langkah krusial dalam memastikan perlindungan data pribadi pasien di era digital. Rumah sakit perlu berinvestasi pada sistem teknologi informasi yang andal dan terstandarisasi, seperti penggunaan server yang terenkripsi, sistem keamanan berlapis (multi-layered security), serta perangkat lunak antivirus dan firewall terbaru. Selain itu, perlu dibangun sistem pencadangan (backup) dan pemulihan data (disaster recovery) untuk mengantisipasi kerusakan atau serangan siber. Sistem ini harus didukung oleh kebijakan keamanan siber yang komprehensif dan penerapan teknologi seperti autentikasi ganda, log akses, serta pemantauan sistem secara real-time agar seluruh aktivitas terhadap data dapat terdeteksi dan dilacak. Langkah ini tidak hanya memperkuat kepercayaan publik terhadap pelayanan rumah sakit, tetapi juga menjadi wujud konkret dari kepatuhan terhadap peraturan perlindungan data pribadi yang berlaku.

#### 2. Pendidikan dan Pelatihan SDM

Peningkatan kapasitas sumber daya manusia sangat penting dalam implementasi regulasi. Rumah sakit perlu memberikan pelatihan rutin kepada tenaga medis, petugas administrasi, dan bagian TI terkait prinsip perlindungan data pribadi, etika medis, dan pemrosesan data sesuai dengan hukum yang berlaku.

**Yudha Aditya Pradana dan Wilma Silalahi**  
*Implementasi dan Tantangan Regulasi Perlindungan Data Pribadi Pasien di Era Digital pada Rumah Sakit*

Pelatihan ini tidak hanya bersifat teknis tetapi juga etis dan hukum agar seluruh personel memiliki kesadaran yang utuh terhadap pentingnya perlindungan data pasien. Pendidikan dan pelatihan sumber daya manusia (SDM) merupakan aspek fundamental dalam menunjang keberhasilan implementasi regulasi perlindungan data pribadi pasien. Tenaga kesehatan, staf administrasi, hingga petugas teknologi informasi di rumah sakit harus dibekali pemahaman menyeluruh mengenai prinsip-prinsip dasar privasi, ketentuan hukum yang berlaku seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta etika pengelolaan informasi medis. Pelatihan ini harus bersifat berkelanjutan dan adaptif terhadap perkembangan teknologi, mencakup simulasi ancaman siber, tata cara pelaporan insiden kebocoran data, serta prosedur penanganan akses ilegal. Dengan membentuk budaya sadar privasi dan meningkatkan kompetensi SDM, rumah sakit dapat meminimalisasi risiko pelanggaran hukum sekaligus menjaga kepercayaan pasien dalam sistem pelayanan kesehatan digital.

3. Penunjukan Data Protection Officer (DPO)

UU PDP mengatur bahwa setiap pengendali data pribadi yang melakukan pemrosesan data dalam skala besar atau sensitif wajib menunjuk Data Protection Officer (DPO). Dalam konteks rumah sakit, DPO bertugas untuk memastikan kepatuhan terhadap UU PDP, mengawasi pengelolaan data, serta menjadi penghubung antara rumah sakit dengan otoritas pengawas. Dengan adanya DPO, rumah sakit akan memiliki pengawasan internal yang lebih efektif dan struktur manajemen risiko yang lebih baik terhadap pelanggaran data pribadi.

Penunjukan DPO merupakan langkah strategis yang wajib dilakukan oleh rumah sakit sebagai bentuk kepatuhan terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. DPO bertanggung jawab atas pengawasan kepatuhan terhadap pengelolaan data pribadi, termasuk merancang kebijakan perlindungan data, melakukan audit internal, memberikan rekomendasi atas potensi risiko, serta menjadi penghubung antara rumah sakit dan otoritas perlindungan data. Dalam konteks rumah sakit, DPO juga berperan penting dalam memastikan bahwa data pasien, terutama rekam medis elektronik, dikelola dengan prinsip kehati-hatian dan tidak disalahgunakan oleh pihak yang tidak berwenang.

Oleh karena itu, pemilihan DPO harus mempertimbangkan kompetensi teknis dan pemahaman hukum yang memadai agar peran ini dapat dijalankan secara profesional dan efektif dalam mendukung tata kelola data pribadi yang aman di era digital.

#### 4. Penyusunan SOP dan Audit Berkala

Rumah sakit perlu menyusun dan menetapkan standar operasional prosedur (SOP) terkait perlindungan data pribadi, mulai dari proses pengumpulan data, penyimpanan, pemanfaatan, hingga penghapusan data. SOP tersebut harus disesuaikan dengan prinsip-prinsip perlindungan data dalam UU PDP dan regulasi sektoral. Audit berkala perlu dilakukan, baik secara internal maupun oleh pihak ketiga, untuk mengukur kepatuhan dan mengevaluasi potensi kelemahan sistem.

Penyusunan Standar Operasional Prosedur (SOP) dan audit berkala merupakan instrumen penting dalam menjamin konsistensi dan kepatuhan rumah sakit terhadap regulasi perlindungan data pribadi. SOP harus mencakup seluruh proses pengelolaan data, mulai dari pengumpulan, penyimpanan, penggunaan, hingga pemusnahan data, dengan memperhatikan prinsip transparansi, minimalisasi data, serta keamanan. Prosedur ini wajib disosialisasikan kepada seluruh unit kerja agar menjadi pedoman yang mengikat dan operasional. Selain itu, audit internal maupun eksternal perlu dilakukan secara berkala untuk mengevaluasi efektivitas pelaksanaan SOP, mendeteksi potensi pelanggaran, dan memberikan rekomendasi perbaikan. Dengan adanya SOP yang jelas dan audit yang rutin, rumah sakit dapat meningkatkan akuntabilitas serta mencegah terjadinya kebocoran atau penyalahgunaan data pribadi pasien secara sistematis.

Meskipun Indonesia telah memiliki landasan hukum yang kuat melalui UU PDP dan regulasi sektoral lainnya, implementasi di lapangan masih menghadapi berbagai tantangan serius. Rumah sakit sebagai institusi vital harus melakukan transformasi internal secara menyeluruh, mulai dari peningkatan infrastruktur hingga penguatan tata kelola data. Perlindungan data pribadi pasien bukan hanya soal teknis, tetapi menyangkut hak asasi manusia dan kepercayaan publik terhadap layanan kesehatan. Ke depan, kolaborasi antara pemerintah, rumah sakit, organisasi profesi, dan masyarakat menjadi kunci untuk menciptakan ekosistem kesehatan digital yang aman, adil, dan akuntabel.

### **C. PENUTUP**

Ketentuan hukum positif di Indonesia yang mengatur perlindungan data pribadi pasien di rumah sakit dalam konteks transformasi digital antara lain terdapat dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang mengklasifikasikan data kesehatan sebagai data pribadi sensitif yang wajib dilindungi secara ketat. Selain itu, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan menjamin kerahasiaan informasi medis pasien, serta Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis yang mengatur kewajiban rumah sakit menjaga keamanan rekam medis, baik manual maupun elektronik. Peraturan tersebut menjadi dasar hukum perlindungan data pasien dalam sistem pelayanan kesehatan berbasis digital. Tantangan yang dihadapi rumah sakit dalam mengimplementasikan regulasi perlindungan data pribadi pasien di era digital meliputi:

- a. Keterbatasan infrastruktur teknologi informasi yang aman dan andal, terutama di rumah sakit daerah.
- b. Kurangnya pemahaman tenaga kesehatan tentang kewajiban hukum dan etika privasi data pasien.
- c. Ancaman serangan siber yang meningkat terhadap sistem informasi rumah sakit.
- d. Tumpang tindih dan belum sinkronnya regulasi teknis antara UU PDP, UU Kesehatan, dan peraturan pelaksana lainnya.

Upaya yang dapat dilakukan antara lain:

- a. Peningkatan kapasitas teknologi dan keamanan siber rumah sakit.
- b. Pendidikan dan pelatihan bagi SDM tentang perlindungan data pribadi.
- c. Penunjukan Data Protection Officer (DPO) sesuai amanat UU PDP.
- d. Penyusunan SOP perlindungan data pasien dan audit berkala oleh instansi pengawas.

## **DAFTAR PUSTAKA**

### **Buku**

- Amelia, S. 2022. *Etika Privasi Data Pasien dalam Praktek Kesehatan Digital*. Yogyakarta: Gajah Mada Press.
- Marzuki, Peter Mahmud. 2014. *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group.

### **Publikasi**

- Agustina, R.. *Harmonisasi Regulasi Perlindungan Data di Sektor Kesehatan*. Jurnal Legislasi Indonesia. Vol.19. No.1 (2022).
- Agustina, R.. *Sinkronisasi Regulasi Perlindungan Data di Sektor Kesehatan*. Jurnal Legislasi Nasional. Vol.11. No.3 (2023).
- Darmawan, F.. *Transforamsi Digital Layanan Kesehatan dan Perlindungan Data Pasien*. Jurnal Hukum Kesehatan. Vol.4. No.1 (2022).
- Hardiansyah, F.. *Kebutuhan Harmonisasi Regulasi Perlindungan Data di Sektor Kesehatan*. Jurnal Legislasi Nasional. Vol.4. No.1 (2023).
- Indriyani, R.. *Digitalisasi Sistem Informasi Rumah Sakit dan Perlindungan Data Pasien*. Jurnal Hukum Kesehatan. Vol.3. No.2 (2022).
- Mulyadi, R.. *Audit Kepatuhan Perlindungan Data di Fasilitas Layanan Kesehatan*. Jurnal Hukum Siber. Vol.6. No.3 (2023).
- Nurhayati, D.. *Kesiapan SIMRS di Rumah Sakit Daerah*. Jurnal Informatika Kesehatan. Vol.3. No.1 (2022).
- Yusuf, M.. *Perlindungan Data Pasien di Era Digitalisasi Rumah Sakit*. Jurnal Hukum & Kesehatan. Vol.8. No.2 (2023).

### **Sumber Hukum**

- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan.
- Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis.