



ANALISIS PERBANDINGAN REGULASI DAN PERLINDUNGAN HUKUM ATAS PRIVASI DATA PASIEN DI TIGA NEGARA ASIA TENGGARA (INDONESIA, SINGAPURA, DAN LAOS)

Heri Heriyanto

Universitas Nusa Putra

heri.heriyanto@nusaputra.ac.id

Abstrak

Legislasi dan perlindungan hukum terhadap privasi data pasien dalam sistem kesehatan elektronik di Indonesia, Singapura, dan Laos akan dibandingkan dalam penelitian ini. Analisis kali ini menyoroti kekuatan dan kelemahan kerangka kerja peraturan, mengidentifikasi tantangan, dan menyarankan arah masa depan untuk meningkatkan privasi data pasien. Temuan ini mengungkapkan bahwa meskipun ketiga negara telah menetapkan undang-undang dan badan pengatur untuk menangani privasi data pasien, Singapura menonjol karena kerangka kerjanya yang komprehensif dan kuat. Undang-Undang Perlindungan Data Pribadi (PDPA) Singapura, yang didukung oleh langkah-langkah penegakan hukum yang efektif, membahas beberapa masalah perlindungan data dan hak privasi yang berbeda. Meskipun upaya telah dilakukan oleh Indonesia dan Laos untuk mengatur privasi data pasien, masih ada ruang untuk perbaikan, terutama dalam metode penegakan hukum dan kepatuhan terhadap standar internasional. Tantangan yang teridentifikasi termasuk sumber daya yang terbatas, kesenjangan kesadaran dan kepatuhan, risiko keamanan siber, dan pembagian data lintas batas. Beberapa arahan untuk masa depan termasuk memperkuat mekanisme penegakan hukum, meningkatkan kolaborasi internasional untuk menyelaraskan standar perlindungan data, mempromosikan tata kelola data dan akuntabilitas dalam organisasi perawatan kesehatan, meningkatkan kesadaran publik dan memberdayakan pasien, serta terus mengevaluasi dan mengadaptasi kerangka kerja peraturan untuk mengatasi risiko yang terus berkembang dan kemajuan teknologi.

Kata Kunci: *privasi data pasien, sistem kesehatan elektronik, regulasi, perlindungan hukum, analisis komparatif*

Abstract

Legislation and legal protection of patient data privacy in e-health systems in Indonesia, Singapore, and Laos will be compared in this study. The present analysis highlights the strengths and weaknesses of the regulatory framework, identifies challenges, and suggests future directions to improve patient data privacy of patient. The findings reveal that while all three countries have established laws and regulatory bodies to address patient data privacy, Singapore stands out for its comprehensive and robust framework. Singapore's Personal Data Protection Act (PDPA), backed by effective enforcement measures, addresses several different data protection and privacy rights issues. While efforts have been made by Indonesia and Laos to regulate patient data privacy, there is still room for improvement, particularly in enforcement methods and compliance with international standards. Identified challenges include limited resources, awareness and compliance gaps, cybersecurity risks, and cross-border data sharing. Some directions for the future include strengthening enforcement mechanisms, increasing international collaboration to harmonize data protection standards, promoting data governance and accountability within healthcare organizations, increasing public awareness and empowering patients, and continuously evaluating and adapting regulatory frameworks to address evolving risks and technological advancements.

Keywords: *patient data privacy, electronic health systems, regulation, legal protection, comparative analysis*

@Jurnal Ners Prodi Sarjana Keperawatan & Profesi Ners FIK UP 2023

✉ Corresponding author :

Address : Jl. Raya Cibolang No.21 Cisaat Sukabumi 43152 Indonesia

Email : heri.heriyanto@nusaputra.ac.id

Phone : 089689961967

PENDAHULUAN

Keberadaan sistem informasi di era digital ini sangat diperlukan untuk menunjang pemerataan sistem informasi di semua bidang, termasuk dalam bidang Kesehatan (Nugraha et al., 2023). Penyebaran sistem kesehatan elektronik yang luas dalam beberapa tahun terakhir telah mengubah lanskap perawatan kesehatan dengan memungkinkan penyimpanan, pertukaran, dan pengambilan data pasien yang lebih efektif. Privasi data telah dipengaruhi oleh peningkatan teknologi dengan cara yang menguntungkan dan negatif. Di satu sisi, teknologi telah memungkinkan untuk mengembangkan alat peningkatan privasi yang dapat melindungi informasi pribadi dari akses dan penggunaan ilegal (Eckhoff & Wagner, 2017; Sagioglu & Sinanc, 2013). Sebagai contoh, desain jaringan 5G dapat memanfaatkan teknologi blockchain untuk mengenkripsi data antar node, sehingga mengurangi risiko keamanan (William dkk., 2022). Analisis data besar juga dapat digunakan di kota pintar untuk mengidentifikasi dan mengurangi masalah privasi (Eckhoff & Wagner, 2017). Di sisi lain, ancaman dan tantangan privasi baru juga muncul akibat kemajuan teknologi. Misalnya, kekhawatiran tentang privasi pasien telah disoroti oleh meningkatnya volume data yang dikumpulkan dan dipertukarkan di sektor perawatan kesehatan (Meinert dkk., 2018; Yarali dkk., 2020). Penggunaan media sosial dan platform daring lainnya juga mengakibatkan pengumpulan dan pembagian data pribadi tanpa sepengetahuan atau persetujuan dari pengguna (Harrigan et al., 2020; Teng dkk., 2022). Masyarakat yang pada dasarnya tidak setara dapat tercipta sebagai akibat dari penggunaan teknologi di kota pintar, yang juga dapat mengakibatkan kurangnya perlindungan privasi, diskriminasi, dan segregasi sosial (Eckhoff & Wagner, 2017). Setiap penduduk tidak memiliki pilihan selain menjadi komponen digital dari kota masa depan sebagai akibat dari penyebaran aplikasi dan sensor di kota pintar, yang dapat mengakibatkan hilangnya kedaulatan data dan kontrol atas informasi pribadi (Eckhoff & Wagner, 2017). Kesimpulannya, kemajuan teknologi telah menghasilkan banyak hal positif, tetapi juga menghasilkan ancaman dan kesulitan privasi yang baru. Untuk melindungi privasi individu di era digital, sangat penting untuk terus menciptakan teknologi dan peraturan yang meningkatkan privasi.

Secara global, melindungi privasi data adalah masalah yang krusial, dan banyak negara telah mengesahkan undang-undang untuk melakukannya. Berbagai komitmen internasional dan regional menawarkan kerangka kerja untuk perlindungan privasi data, sementara landasan hukum untuk perlindungan privasi data berbeda-beda di setiap negara. Peraturan Perlindungan Data Umum (GDPR) Uni Eropa (UE) adalah komitmen paling signifikan di seluruh dunia untuk perlindungan privasi data (Goddard, 2017). GDPR adalah undang-undang menyeluruh yang menguraikan pedoman pengumpulan, penggunaan, dan penyimpanan data pribadi. Di mana pun organisasi tersebut berbasis, peraturan ini berlaku untuk semua organisasi yang memproses data pribadi warga negara Uni Eropa. Mengikuti GDPR, orang memiliki beberapa hak, termasuk kemampuan untuk melihat data pribadi mereka, menghapusnya, dan menolak pemrosesannya. Pedoman PBB untuk Regulasi File Data Pribadi Terkomputerisasi dan Konvensi Dewan Eropa untuk Perlindungan Individu tentang Pemrosesan Otomatis Data Pribadi adalah dua komitmen internasional tambahan yang menawarkan kerangka kerja untuk perlindungan privasi data (Greenleaf & Cottier, 2020). Terdapat perjanjian regional yang menawarkan kerangka kerja untuk perlindungan privasi data sebagai tambahan dari komitmen internasional. Misalnya, Uni Afrika (AU) memberlakukan Konvensi Malabo (juga dikenal sebagai Konvensi Uni Afrika tentang Keamanan Siber dan Perlindungan Data Pribadi), yang menguraikan pedoman untuk pengumpulan, penggunaan, dan penyimpanan data pribadi di Afrika (Greenleaf & Cottier, 2020). Hanya sepertiga dari ratifikasi yang diperlukan untuk Konvensi Malabo yang telah diperoleh, tetapi memiliki potensi untuk menjadi komitmen regional yang signifikan terhadap perlindungan privasi data di Afrika. Seiring dengan GDPR dan Petunjuk ePrivacy, Uni Eropa telah membuat janji regional untuk menjaga privasi data (Goddard, 2017; Intersoft Consulting, 2018). Aturan untuk perlindungan data pribadi dalam komunikasi elektronik, seperti email dan pesan instan, diuraikan dalam Petunjuk ePrivacy.

Secara global, ada banyak kekhawatiran tentang bagaimana privasi data pasien dilindungi dalam sistem kesehatan elektronik. Kekhawatiran privasi pasien dapat muncul karena keselamatan pasien tidak ditangani di Asia Tenggara seperti halnya di negara-negara Barat (Kang dkk., 2021). Sebanyak 142 negara akan memiliki undang-

undang privasi data pada akhir tahun 2019 berkat 62 negara baru yang memberlakukannya selama dekade 2010-2019 (Greenleaf, 2020). Namun, salah satu kendala utama untuk mendigitalkan informasi kesehatan pasien secara penuh dalam rekam medis elektronik (EMR) adalah kurangnya interoperabilitas (Shrivastava et al., 2021). Metode yang diusulkan untuk memastikan keamanan dan privasi rekam medis elektronik adalah sistem yang dikendalikan oleh pasien yang menggunakan teknik pseudonimisasi (Rai, 2022). Selain itu, model data yang melampirkan tingkat keamanan pada data itu sendiri, seperti yang dinyatakan dalam bentuk XML, telah diusulkan untuk meningkatkan keamanan dan privasi data kesehatan (Asija & Nallusamy, 2014). Secara keseluruhan, masih ada masalah dengan interoperabilitas dan budaya di Asia Tenggara yang memprioritaskan keselamatan pasien meskipun ada undang-undang dan solusi yang telah disajikan untuk menjaga privasi data pasien dalam sistem kesehatan elektronik.

Tabel 1. Indeks CGI 2020

Negara	Skor	Peringkat Dunia	Peringkat Asia Pasifik
Singapura	98,52	4	1
Indonesia	94,88	24	6
Laos	20,34	131	25

Sumber : Indeks GCI (2020)

Komponen penting dalam menyediakan layanan kesehatan di era digital saat ini adalah menjaga privasi data pasien dalam sistem kesehatan elektronik. Mengamankan kerahasiaan dan keamanan data ini sangat penting karena organisasi layanan kesehatan semakin mengandalkan sistem elektronik untuk menyimpan dan mengkomunikasikan informasi pasien yang sensitif. Negara-negara Asia Tenggara, di mana penyebaran sistem kesehatan elektronik telah meningkat secara signifikan dalam beberapa tahun terakhir, harus memberikan perhatian khusus terhadap hal ini. Penelitian GCI menunjukkan bahwa negara-negara Asia Tenggara menunjukkan rentang yang luas dalam indeks, yang menunjukkan bahwa ada ketidaksetaraan dalam tingkat perkembangan mereka. sehingga menjadi dasar untuk penelitian ini.

Berdasarkan sistem perawatan kesehatan yang berbeda, tingkat adopsi sistem eHealth, dan kepentingan regional, tiga negara Asia Tenggara yang termasuk dalam penelitian ini dipilih. Negara-negara ini menawarkan kesempatan untuk

mempelajari perbedaan lingkungan legislatif dan menyelidiki potensi praktik terbaik untuk melindungi privasi data pasien. Tujuan dari penelitian ini adalah untuk ; (1) mengetahui gambaran umum sistem kesehatan elektronik di Indonesia, Singapura, dan RDR Laos, (2) mengetahui kerangka kerja dan kebijakan untuk privasi data pasien yang sudah ada di Indonesia, Singapura, dan RDR Laos, (3) melakukan analisis komparatif terhadap hukum dan perlindungan hukum untuk privasi data pasien di Indonesia, Singapura, dan RDR Laos dalam sistem kesehatan elektronik, dan juga (4) mengeksplorasi tantangan dan arah masa depan perlindungan hukum untuk privasi data pasien di Indonesia, Singapura, dan RDR Laos dalam sistem kesehatan elektronik

METODE

Penelitian yang dilakukan adalah penelitian tinjauan literatur dengan metode analisis deskriptif. Selain itu, penelitian ini juga menggunakan metodologi komparatif, yaitu membandingkan hukum dan peraturan di Singapura, Indonesia, dan Laos dalam hal perlindungan data pribadi. Tinjauan literatur akan dilakukan untuk penelitian ini untuk membandingkan hukum dan perlindungan hukum untuk data pasien dalam sistem kesehatan elektronik di tiga negara. Deskripsi fakta dan fenomena terkait regulasi dan perlindungan hukum terhadap data pasien di ketiga negara tersebut dapat memberikan gambaran yang komprehensif mengenai tingkat keamanan siber di ketiga negara tersebut.

HASIL DAN PEMBAHASAN

a. Gambaran Umum Sistem Kesehatan Elektronik di Indonesia, Singapura, dan RDR Laos

- **Indonesia**

Di Indonesia, penerapan sistem kesehatan elektronik masih dalam tahap awal, dengan upaya berkelanjutan untuk memperkuat infrastruktur kesehatan dan inisiatif kesehatan digital. Pemerintah memahami pentingnya penerapan rekam kesehatan elektronik (EHR) dan mendorong interoperabilitas di antara fasilitas kesehatan. Namun, integrasi dan implementasi sistem kesehatan elektronik masih terbatas di seluruh negeri, terutama di daerah pedesaan. Pertukaran Informasi

Kesehatan Nasional (National Health Information Exchange/NHI), yang akan memudahkan penyedia layanan kesehatan untuk berbagi data, merupakan salah satu inisiatif yang didorong oleh Kementerian Kesehatan untuk mendorong penggunaan teknologi dalam penyediaan layanan kesehatan. Terlepas dari masalah infrastruktur, keuangan, dan pengembangan kapasitas, Indonesia membuat kemajuan dalam mengembangkan sistem e-health untuk meningkatkan akses dan kualitas layanan kesehatan.

- **Singapura**

Singapura telah membangun sistem *e-health* yang canggih dan komprehensif, menjadikannya sebagai pelopor layanan kesehatan digital. Penggunaan dan integrasi sistem kesehatan elektronik yang meluas merupakan konsekuensi dari pengeluaran yang signifikan dalam infrastruktur dan teknologi informasi kesehatan. Elemen-elemen kunci dari sistem kesehatan elektronik Singapura meliputi National Electronic Health Record (NEHR), yang memungkinkan pertukaran data pasien secara aman di seluruh penyedia layanan kesehatan, dan platform HealthHub, yang memungkinkan masyarakat untuk melihat catatan kesehatan mereka dan mengelola janji temu secara online. Pemerintah juga telah mempromosikan *telemedicine* dan pemantauan jarak jauh, yang meningkatkan perawatan dan kenyamanan pasien. Sistem eHealth Singapura telah memberikan kontribusi yang signifikan terhadap koordinasi perawatan kesehatan yang lebih baik, efisiensi, dan hasil yang lebih baik bagi pasien.

- **Republik Demokratik Rakyat (RDR) Laos**

RDR Laos menciptakan dan memperluas sistem kesehatan elektroniknya untuk meningkatkan layanan kesehatan dan mengatasi kendala geografis. Manfaat potensial dari digitalisasi catatan kesehatan dan manajemen data yang lebih baik dalam pengaturan layanan kesehatan telah diakui oleh negara ini. Pemerintah telah mulai bekerja pada catatan kesehatan elektronik dan sistem informasi kesehatan digital,

untuk meningkatkan aksesibilitas data, akurasi, dan efisiensi dalam pemberian layanan kesehatan. Namun, implementasi sistem kesehatan elektronik di Laos masih dalam tahap awal, dengan cakupan yang terbatas dan kendala infrastruktur, terutama di lokasi pedesaan dan terpencil. Upaya-upaya sedang dilakukan untuk membangun infrastruktur kesehatan digital, membangun kapasitas di antara para profesional kesehatan, dan mempromosikan interoperabilitas sistem informasi kesehatan.

Meskipun terdapat perbedaan dalam tingkat implementasi dan adopsi, terdapat beberapa tema umum yang sama di antara sistem e-Kesehatan di Indonesia, Singapura, dan Laos. Nilai kesehatan digital dalam meningkatkan layanan kesehatan, upaya untuk meningkatkan interoperabilitas dan pertukaran data di seluruh penyedia layanan kesehatan, dan penerapan rekam kesehatan elektronik untuk koordinasi perawatan pasien yang lebih baik adalah beberapa dari tema-tema tersebut. Ketiga negara tersebut menghadapi masalah infrastruktur, keuangan, keamanan data, masalah privasi, dan kebutuhan akan pengembangan kapasitas profesional kesehatan. Namun, mereka bekerja keras untuk memperluas sistem kesehatan elektronik mereka untuk mengatasi masalah-masalah ini dan meningkatkan hasil perawatan kesehatan. Pemeriksaan terhadap sistem eHealth di Indonesia, Singapura, dan Laos memberikan dasar untuk memahami lingkungan di mana undang-undang privasi data pasien berlaku. Hal ini berfungsi sebagai dasar untuk analisis komparatif hukum privasi data pasien dan perlindungan hukum di berbagai negara, yang membantu dalam mengidentifikasi kekuatan, kekurangan, dan potensi pengembangan dalam memastikan privasi pasien dalam sistem e-kesehatan.

- b. Kerangka Kerja Regulasi untuk Privasi Data Pasien di Indonesia, Singapura, dan RDR Laos**

- **Indonesia**

Berbagai undang-undang dan peraturan mengatur privasi data pasien di Indonesia. Undang-undang utama yang mengatur privasi dan keamanan informasi kesehatan adalah Undang-Undang tentang Privasi dan Keamanan Informasi Kesehatan, yang menetapkan prinsip-prinsip dan peraturan untuk perlindungan data kesehatan.

Pentingnya izin, kerahasiaan, keamanan data, dan hak-hak pasien untuk mengakses dan mengontrol informasi kesehatan mereka ditekankan dalam peraturan ini. Selain itu, Kementerian Kesehatan memainkan peran penting dalam mengatur privasi data kesehatan dengan mengeluarkan pedoman, surat edaran, dan standar perlindungan data. Namun, karena sumber daya yang terbatas dan tingkat pemahaman yang bervariasi di antara para praktisi kesehatan, penerapan dan penegakan peraturan ini dapat menemui hambatan.

- **Singapura**

Personal Data Protection Act (PDPA), yang merupakan kerangka kerja peraturan utama yang berlaku di Singapura untuk melindungi privasi data pasien, bertanggung jawab atas bidang hukum ini. PDPA menciptakan kerangka kerja yang menyeluruh untuk mengumpulkan, menggunakan, mengungkapkan, dan melindungi informasi pribadi, termasuk informasi yang berhubungan dengan kesehatan. PDPA menetapkan hak-hak seseorang untuk mengakses dan mengubah informasi mereka serta hak-hak mereka untuk memberikan persetujuan atas pengumpulan dan penggunaan data mereka. PDPA mengamanatkan agar perusahaan menerapkan langkah-langkah keamanan yang diperlukan untuk melindungi data pribadi dari akses atau pengungkapan yang tidak sah. Melalui investigasi, audit, dan penyebaran saran dan nasihat, Komisi Perlindungan Data Pribadi (PDPC) bertugas menegakkan PDPA dan memastikan kepatuhan.

- **RDR Laos**

Undang-Undang Perlindungan Data Elektronik, yang menyediakan kerangka hukum untuk perlindungan data elektronik, termasuk informasi kesehatan, mengatur privasi data pasien di Laos. Undang-undang ini mendefinisikan hak dan kewajiban pengontrol data dan subjek data, menekankan pentingnya persetujuan, kerahasiaan, dan pelaksanaan langkah-langkah keamanan. Pusat Internet Nasional Laos bertanggung jawab untuk mengatur perlindungan data di negara ini, serta meningkatkan kesadaran dan menegakkan aturan privasi data. Namun, sangat penting untuk diingat bahwa lingkungan peraturan di Laos masih terus berubah, dan pedoman tambahan serta peraturan khusus untuk privasi data kesehatan mungkin diperlukan.

Beberapa kesamaan dan variasi muncul ketika memeriksa kerangka kerja peraturan untuk privasi data pasien di Indonesia, Singapura, dan Laos. Ketiga negara tersebut mengakui pentingnya perlindungan data pasien dan telah mengesahkan undang-undang untuk mengatasi masalah privasi data. Meskipun aturan dan proses khusus untuk mendapatkan persetujuan mungkin berbeda, persetujuan adalah aspek umum dari peraturan tersebut. Keamanan data diprioritaskan di ketiga negara tersebut, meskipun tingkat saran dan detailnya berbeda-beda. PDPA di Singapura terkenal karena pendekatannya yang komprehensif terhadap perlindungan data, termasuk prinsip-prinsip yang jelas, langkah-langkah penegakan hukum, dan otoritas khusus untuk mengawasi kepatuhan. Sebaliknya, Indonesia dan Laos mungkin akan mendapatkan manfaat dari kejelasan, saran, dan alat penegakan hukum yang lebih baik untuk menjamin bahwa undang-undang privasi data diimplementasikan secara efektif.

Kesesuaian kerangka kerja legislatif dengan norma dan pedoman internasional untuk perlindungan data pasien merupakan komponen penting. Peraturan Perlindungan Data Umum (GDPR) Uni Eropa, serta standar dari organisasi seperti Organisasi Kesehatan Dunia (WHO) dan Organisasi Internasional untuk Standardisasi (ISO), menjadi tolok ukur kebijakan perlindungan data. PDPA di Singapura sangat selaras dengan standar di seluruh dunia, yang mencakup nilai-nilai seperti akuntabilitas, keterbukaan, dan hak-hak individu untuk mengatur data mereka. Dalam hal mencocokkan peraturan lokal dengan standar internasional ini, Indonesia dan Laos mungkin masih memiliki ruang untuk perbaikan, terutama di bidang-bidang seperti persyaratan pelaporan pelanggaran data dan langkah-langkah penegakan hukum.

Kerangka kerja peraturan Indonesia, Singapura, dan Laos untuk privasi data pasien menunjukkan dedikasi negara-negara ini untuk melindungi informasi pasien dalam sistem kesehatan elektronik. Meskipun setiap negara telah memberlakukan undang-undang dan membentuk badan pengawas untuk mengawasi privasi data, terdapat perbedaan dalam hal cakupan, mekanisme penegakan hukum, dan keselarasan dengan standar internasional. Memahami kerangka kerja peraturan ini sangat penting untuk menganalisis kemampuan perlindungan privasi data pasien dan mengidentifikasi area yang perlu ditingkatkan dalam konteks sistem eHealth.

Analisis Perbandingan Kerangka Kerja Legislatif Peraturan Privasi Data Pasien

Dalam hal kerangka kerja legislatif, Indonesia, Singapura, dan Laos telah mengesahkan undang-undang untuk mengatur privasi data pasien dalam sistem eHealth. Undang-Undang tentang Privasi dan Keamanan Informasi Kesehatan di Indonesia menetapkan prinsip-prinsip dan peraturan untuk perlindungan data kesehatan. Undang-Undang Perlindungan Data Pribadi (PDPA) di Singapura menetapkan kerangka kerja yang komprehensif untuk pengumpulan, penggunaan, dan perlindungan data pribadi, termasuk informasi kesehatan. Laos memiliki Undang-Undang Perlindungan Data Elektronik yang menciptakan kerangka hukum untuk mengamankan data elektronik, terutama informasi kesehatan. Meskipun ketiga negara tersebut memiliki undang-undang yang membahas privasi data pasien, PDPA Singapura adalah yang paling komprehensif dan terperinci, yang mencakup berbagai perlindungan data dan hak privasi.

- **Otoritas Perlindungan Data**

Setiap negara telah menunjuk otoritas yang bertanggung jawab atas perlindungan data dan privasi. Komisi Perlindungan Data Pribadi (Personal Data Protection Commission/PDPC) adalah otoritas pengawas di Singapura, yang bertanggung jawab untuk menegakkan PDPA dan mendorong kepatuhan. PDPC dapat melakukan investigasi dan menjatuhkan hukuman atas pelanggaran. Kementerian Kesehatan di Indonesia bertanggung jawab untuk mengatur privasi data kesehatan dan melaksanakan Undang-Undang tentang Privasi dan Keamanan Informasi Kesehatan. Pusat Internet Nasional Laos bertanggung jawab atas perlindungan data di Laos, namun perannya dalam menegakkan undang-undang privasi data mungkin memerlukan lebih banyak perbaikan. PDPC di Singapura terkenal dengan otoritas dan mekanisme penegakan hukumnya yang mapan, yang memastikan lingkungan peraturan yang solid untuk perlindungan data pasien.

- **Mekanisme Persetujuan**

Metode persetujuan sangat penting dalam aturan privasi data pasien. Di Singapura, Personal Data Protection Act (PDPA) mewajibkan organisasi untuk meminta persetujuan eksplisit dan terinformasi dari individu sebelum mengumpulkan, menggunakan, atau mengungkapkan data

mereka, termasuk informasi kesehatan. PDPA juga menekankan pentingnya mengizinkan orang untuk menarik izin. Hukum persetujuan tidak terlalu eksplisit di Indonesia dan RDR Laos, dengan skenario tertentu yang mengandalkan persetujuan yang diasumsikan. Namun, kedua negara tersebut memahami pentingnya persetujuan dalam melindungi privasi pasien. Undang-Undang Perlindungan Data Pribadi (PDPA) Singapura menetapkan standar yang lebih tinggi untuk izin, dengan menekankan kepemilikan individu atas data mereka.

- **Langkah-langkah Keamanan Data**

Ketiga negara mengakui perlunya langkah-langkah keamanan data dalam sistem kesehatan elektronik untuk melindungi informasi pasien. Undang-Undang Perlindungan Data Pribadi (PDPA) Singapura memberikan rekomendasi dan peraturan terperinci bagi perusahaan untuk menetapkan langkah-langkah keamanan yang tepat untuk melindungi data pribadi dari akses, pengungkapan, dan kehilangan yang tidak sah. Hal ini menekankan pentingnya aturan keamanan data, kontrol akses, enkripsi, dan penilaian keamanan data secara berkala. Indonesia dan Laos juga memiliki aturan keamanan data, tetapi kriteria dan prosedur spesifiknya tidak terlalu luas. PDPA Singapura meningkatkan standar perlindungan keamanan data, dengan menganjurkan kerangka kerja perlindungan yang lebih kuat untuk data pasien.

- **Transfer Data Lintas Batas**

Peraturan transfer data lintas batas mengatur pergerakan data pasien di luar otoritas negara. Singapura telah mengambil pendekatan kecukupan, yang mengizinkan data pribadi ditransfer ke negara-negara dengan peraturan perlindungan data yang sebanding. Metode ini memastikan bahwa data tetap aman bahkan ketika dipindahkan secara global. Sebelum memindahkan data ke luar yurisdiksi masing-masing, Indonesia dan Laos mewajibkan pengeksport data untuk menjaga keamanan yang tepat dan memperoleh persetujuan. Pengamanan ini dirancang untuk melindungi data pasien saat data tersebut berpindah melintasi perbatasan. Strategi kecukupan Singapura menunjukkan pendekatan proaktif terhadap transfer data lintas batas, yang memberikan tingkat perlindungan privasi pasien yang lebih tinggi.

- **Kekuatan dan Kelemahan Komparatif**

Analisis komparatif menunjukkan kekuatan dan kelemahan peraturan privasi data pasien di Indonesia, Singapura, dan Laos. PDPA Singapura menonjol karena pendekatannya yang komprehensif, yang mencakup berbagai aspek perlindungan data dan hak privasi. Pembentukan PDPC sebagai otoritas regulasi dan mekanisme penegakan hukumnya yang kuat berkontribusi pada kerangka kerja regulasi yang kuat. Indonesia dan Laos telah melakukan upaya untuk mengatur privasi data pasien, tetapi mungkin ada kebutuhan untuk pengembangan lebih lanjut dan penyesuaian dengan standar internasional. Kejelasan dan kelengkapan peraturan, persyaratan persetujuan, langkah-langkah keamanan data, dan mekanisme transfer data lintas batas dapat menjadi area yang perlu ditingkatkan untuk Indonesia dan RDR Laos. Pemeriksaan komparatif terhadap peraturan privasi data pasien mengungkapkan kekuatan dan kelemahan kerangka hukum di Indonesia, Singapura, dan Laos. Temuan ini dapat membantu pemerintah, organisasi layanan kesehatan, dan pemangku kepentingan lainnya untuk mengidentifikasi area yang perlu diperbaiki dan meningkatkan perlindungan privasi data pasien dalam sistem e-kesehatan.

- c. **Perlindungan Hukum atas Privasi Data Pasien di Indonesia, Singapura, dan RDR Laos**

- **Akses dan Kontrol Data**

Pasien memiliki hak hukum untuk mengakses dan mengontrol informasi kesehatan mereka yang disimpan dalam sistem kesehatan elektronik di ketiga negara tersebut. Individu di Indonesia memiliki hak untuk melihat catatan kesehatan mereka dan meminta koreksi atau penambahan informasi di bawah Undang-Undang tentang Privasi dan Keamanan Informasi Kesehatan. Individu di Singapura memiliki hak di bawah PDPA untuk mengakses data pribadi mereka dan meminta koreksi atau pencabutan izin. Undang-Undang Perlindungan Data Elektronik di Laos menghormati hak-hak individu untuk mengakses dan mengatur data kesehatan elektronik mereka. Perlindungan hukum ini dimaksudkan untuk memberdayakan pasien dan memungkinkan mereka menangani informasi kesehatan mereka dengan baik.

- **Kerahasiaan dan Non-Pengungkapan**

Elemen utama dari perlindungan privasi pasien adalah kerahasiaan dan kerahasiaan data pasien. Undang-Undang Indonesia tentang Kerahasiaan dan Keamanan Informasi Kesehatan menekankan kewajiban praktisi kesehatan untuk menjaga kerahasiaan informasi kesehatan dan melarang pengungkapan yang tidak sah. Demikian pula, PDPA di Singapura mewajibkan perusahaan untuk menjaga kerahasiaan data pribadi dan menghindari pengungkapan yang tidak sah. Undang-Undang Perlindungan Data Elektronik di Laos juga mewajibkan pengontrol data untuk melindungi kerahasiaan dan keamanan data kesehatan elektronik. Ketentuan hukum ini berupaya mencegah akses ilegal dan menjaga privasi informasi pasien.

- **Pemberitahuan Pelanggaran Data**

Menangani pelanggaran data merupakan komponen penting dalam melindungi privasi data pasien. PDPA di Singapura mewajibkan orang-orang yang terkena dampak dan PDPC untuk diberitahu tentang pelanggaran data. Organisasi harus memberi tahu individu tentang pelanggaran data apa pun yang dapat mengakibatkan hilangnya atau dampak serius pada data pribadi individu. Indonesia dan RDR Laos belum memiliki ketentuan khusus dalam undang-undang yang ada untuk pemberitahuan pelanggaran data. Namun, penting untuk dicatat bahwa menerapkan prosedur pemberitahuan pelanggaran data dapat mendorong transparansi dan akuntabilitas dalam melindungi privasi data pasien.

- **Hukuman dan Penegakan Hukum**

Ketiga negara memiliki penegakan hukum dan hukuman yang berbeda untuk ketidakpatuhan terhadap aturan privasi data pasien. PDPC di Singapura memiliki wewenang untuk menegakkan PDPA dan memungut denda atas ketidakpatuhan terhadap undang-undang perlindungan data. PDPC memiliki wewenang untuk melakukan investigasi, mengeluarkan arahan, dan memungut denda untuk pelanggaran PDPA, yang bisa sangat besar. Kementerian Kesehatan di Indonesia bertanggung jawab untuk menegakkan Undang-Undang Privasi dan Keamanan Informasi Kesehatan, namun mekanisme penegakan hukum dan hukuman untuk ketidakpatuhan bervariasi. Pusat Internet Nasional Laos bertanggung jawab atas

perlindungan data, namun metode penegakan dan hukuman mungkin perlu ditingkatkan.

- **Transfer Data Lintas Batas dan Kerja Sama Internasional**

Privasi data pasien dilindungi secara hukum dalam transfer data lintas batas dan kerja sama internasional. Undang-Undang Perlindungan Data Pribadi (PDPA) Singapura mencakup aturan untuk mentransfer data pribadi ke negara-negara dengan undang-undang perlindungan data yang sebanding, memastikan bahwa data diamankan saat dikirim ke luar negeri. Sebelum mengekspor data ke luar yurisdiksi mereka, Indonesia dan Laos mewajibkan pengekspor data untuk menjaga keamanan yang tepat dan mendapatkan persetujuan. Langkah-langkah ini sejalan dengan standar internasional dan menunjukkan komitmen untuk melindungi privasi data pasien melintasi batas negara.

- **Keuntungan dan Kerugian Komparatif**

Perbandingan perlindungan hukum terhadap privasi data pasien di Indonesia, Singapura, dan Laos menunjukkan kelebihan dan kekurangan sistem regulasi. Singapura terkenal dengan kerangka kerja peraturannya yang luas, langkah-langkah penegakan hukum yang kuat, dan peraturan pemberitahuan pelanggaran data. Negara ini memiliki aturan yang ketat untuk melindungi privasi data pasien. Meskipun Indonesia dan Laos telah menciptakan perlindungan hukum untuk privasi data pasien, mungkin masih ada kebutuhan untuk perbaikan, seperti mekanisme penegakan hukum yang lebih baik, ketentuan khusus untuk notifikasi pelanggaran data, dan harmonisasi dengan norma-norma internasional.

Perlindungan hukum untuk privasi data pasien dalam rekam kesehatan elektronik diperlukan untuk melindungi hak-hak pasien dan menjaga kepercayaan terhadap sistem perawatan kesehatan. Perlindungan hukum ini, yang meliputi akses dan kontrol data, kerahasiaan, persyaratan izin, pemberitahuan pelanggaran data, mekanisme penegakan hukum, dan kolaborasi internasional, sangat penting dalam menjaga privasi dan keamanan informasi pasien.

Penelitian komparatif mengenai perlindungan legislatif privasi data pasien di Indonesia, Singapura, dan Laos ini memberikan informasi yang signifikan bagi para pembuat kebijakan, organisasi perawatan

kesehatan, dan para pemangku kepentingan yang meneliti kekuatan dan kekurangan dari peraturan yang ada. Penelitian ini mengidentifikasi area untuk pengembangan dan area yang membutuhkan perbaikan untuk melindungi privasi data pasien dengan lebih baik dalam sistem eHealth regional.

Indonesia, Singapura, dan Laos memiliki kerangka hukum yang berbeda untuk melindungi privasi data pasien. Inilah yang kami temukan:

- **Indonesia**

Indonesia memiliki penelitian normatif yang meneliti masalah sosiologis praktis tentang privasi data pasien dan peraturan pemerintah tentang perlindungan data pasien (Natamiharja dkk., 2022). Pandemi Covid-19 telah menuntut penyesuaian dalam pengendalian penularan, termasuk transparansi data. Indonesia membuka data terkait vaksin, booster, dan informasi kesehatan lainnya melalui aplikasi terintegrasi bernama "Peduli Lindungi". Namun, aplikasi ini rentan terhadap kebocoran data karena menggunakan Nomor Induk Kependudukan (NIK) untuk registrasi. Di saat yang sama, aplikasi ini harus digunakan oleh semua orang Indonesia untuk memasuki ruang publik, terutama penerbangan internasional (Natamiharja dkk., 2022).

- **Singapura**

Singapura telah memberlakukan undang-undang privasi data. Personal Data Protection Act (PDPA) mengatur pengumpulan, penggunaan, dan pengungkapan data pribadi oleh organisasi di Singapura. PDPA menetapkan rezim perlindungan data yang terdiri dari berbagai aturan yang mengatur pengumpulan, penggunaan, pengungkapan, dan perlakuan terhadap data pribadi (Greenleaf dkk., 2012).

- **RDR Laos**

Terdapat informasi terbatas tentang perlindungan hukum Laos untuk privasi data pasien. Namun, Masyarakat Ekonomi ASEAN (MEA), yang didirikan pada tahun 2015, memiliki salah satu tujuan e-commerce untuk mengembangkan 'kerangka kerja yang koheren dan komprehensif untuk perlindungan data pribadi' pada tahun 2016-2025, termasuk 'Perlindungan Data Regional dan Prinsip Privasi' (Greenleaf, 2017). Secara keseluruhan, tampaknya Singapura memiliki perlindungan hukum yang lebih komprehensif untuk privasi data pasien dibandingkan dengan Indonesia dan Laos. Namun, perlu dicatat bahwa

Indonesia dan Laos sedang berupaya mengembangkan kerangka kerja untuk perlindungan data pribadi. Penting untuk diingat bahwa kerangka hukum untuk privasi data pasien terus berkembang, dan yang terbaik adalah berkonsultasi dengan ahli hukum untuk mendapatkan informasi terbaru.

d. Tantangan dan Arah Masa Depan

Tantangan dalam perlindungan hukum untuk privasi data pasien, antara lain:

- **Kendala Sumber Daya**

Keterbatasan sumber daya merupakan salah satu masalah utama yang dihadapi ketiga negara dalam menjamin regulasi yang efektif dan perlindungan hukum terhadap privasi data pasien. Mengalokasikan sumber daya keuangan dan manusia yang memadai untuk membangun dan menerapkan kerangka kerja peraturan yang solid, melakukan audit, dan menegakkan kepatuhan bisa jadi sulit. Karena sumber daya yang terbatas, mungkin sulit untuk memantau dan merespons pelanggaran privasi, mengedukasi petugas kesehatan tentang praktik privasi data, dan menciptakan kesadaran publik tentang hak-hak pasien dan perlindungan data.

- **Kepatuhan dan Kesadaran**

Masalah lainnya adalah perbedaan dalam kesadaran dan kepatuhan di seluruh penyedia layanan kesehatan dan organisasi. Menerapkan standar privasi data membutuhkan kesadaran menyeluruh tentang persyaratan hukum serta kemauan untuk mematuhi. Pelanggaran privasi data pasien yang tidak disengaja dapat terjadi karena kurangnya kesadaran dan pemahaman di antara petugas kesehatan. Inisiatif pendidikan dan pelatihan yang berkelanjutan diperlukan untuk meningkatkan kesadaran, pengetahuan, dan kepatuhan terhadap standar perlindungan data.

- **Perkembangan Teknologi dan Ancaman Keamanan Siber**

Kemajuan teknologi yang cepat dalam perawatan kesehatan, seperti catatan kesehatan elektronik, membawa manfaat dan kekhawatiran. Meskipun rekam kesehatan elektronik meningkatkan akses ke informasi kesehatan dan perawatan pasien, namun hal ini juga meningkatkan bahaya ancaman keamanan siber dan pelanggaran data. Mengikuti perkembangan teknologi dan mengatasi masalah keamanan siber memerlukan pemantauan yang berkelanjutan, memperbarui

langkah-langkah keamanan, dan menerapkan kebijakan perlindungan data yang kuat.

- **Pertukaran Data Lintas Batas**

Berbagi data lintas batas menjadi lebih luas dalam industri perawatan kesehatan. Namun, menyelaraskan undang-undang privasi data pasien antar negara bisa jadi sulit. Untuk memastikan bahwa data pasien terlindungi saat dikirim secara global, diperlukan kerja sama internasional, kepatuhan terhadap standar internasional, dan penetapan prosedur untuk berbagi data yang aman.

- **Meningkatkan Mekanisme Penegakan Hukum**

Untuk meningkatkan perlindungan privasi data pasien, prosedur penegakan hukum harus diperkuat. Hal ini mencakup pemberian otoritas pengatur otoritas dan sumber daya yang mereka butuhkan untuk memantau kepatuhan, melakukan investigasi, dan memungut denda atas ketidakpatuhan. Langkah-langkah penegakan hukum yang proaktif dapat berfungsi sebagai pencegah sekaligus mendorong perusahaan untuk menangani privasi dan keamanan data.

- **Meningkatkan Kerja Sama Internasional**

Mengingat sifat berbagi data di seluruh dunia, membina kolaborasi internasional dan menyelaraskan peraturan perlindungan data dapat membantu mengamankan privasi data pasien. Negara-negara dapat berkolaborasi untuk menciptakan kerangka kerja untuk transfer data lintas batas yang aman, mendiskusikan praktik terbaik, dan menyelaraskan kebijakan dengan standar internasional seperti GDPR dan WHO, dan pedoman ISO.

- **Tata Kelola Data dan Promosi Akuntabilitas**

Untuk memastikan privasi data pasien, budaya tata kelola dan akuntabilitas data harus dibangun. Bisnis layanan kesehatan harus menciptakan kerangka kerja tata kelola data yang kuat, menerapkan prinsip-prinsip privasi berdasarkan desain, dan membangun kerangka kerja akuntabilitas. Menunjuk petugas perlindungan data, melakukan audit privasi secara berkala, dan menjaga transparansi dalam metode penanganan data adalah bagian dari hal ini.

- **Pendidikan dan Pemberdayaan Publik**

Sangat penting untuk meningkatkan pengetahuan publik tentang hak privasi data

pasien dan memungkinkan individu untuk melakukan kontrol atas informasi kesehatan mereka. Pasien dapat memperoleh manfaat dari program pendidikan yang membantu mereka memahami hak-hak mereka, pentingnya persetujuan, dan bagaimana menjaga data mereka. Komunikasi yang transparan mengenai prosedur penanganan data dapat membantu masyarakat dan tenaga kesehatan membangun kepercayaan.

- **Evaluasi dan Adaptasi Berkelanjutan**

Untuk mengimbangi kemajuan teknologi dan kekhawatiran yang berkembang, kerangka kerja peraturan untuk privasi data pasien harus terus berkembang. Kerangka kerja legislatif akan terus efektif dalam melindungi privasi data pasien jika legislasi yang ada dievaluasi secara teratur, umpan balik dari para pemangku kepentingan disertakan, dan kekhawatiran yang muncul ditangani. Terakhir, menyelesaikan masalah seperti keterbatasan sumber daya, kesadaran, dan kesenjangan kepatuhan, masalah keamanan siber, dan berbagi data lintas batas akan sangat penting untuk masa depan privasi data pasien dalam sistem e-kesehatan. Memperkuat mekanisme penegakan hukum, meningkatkan kolaborasi internasional, mempromosikan tata kelola dan akuntabilitas data, meningkatkan kesadaran publik, dan mengadaptasi peraturan dengan kebutuhan yang terus berubah, semuanya akan membantu memastikan perlindungan yang efektif terhadap privasi data pasien di Indonesia, Singapura, RDR Laos, dan tempat lainnya.

Arah Masa Depan Perlindungan Hukum untuk Privasi Data Pasien dalam Sistem Kesehatan Elektronik

Perlindungan data pribadi dan medis pasien selalu menjadi topik penting dalam praktik medis, dengan peraturan yang eksplisit. Baik itu hukum perdata dan pidana atau hukum yang mengatur profesi medis, semuanya berupaya melindungi hak asasi manusia yang mendasar. Kerahasiaan data medis dipertahankan bahkan setelah kematian pasien, sebuah aspek yang telah diatur sejak profil profesi medis melalui Sumpah Hipokrates (Dumitrescu, 2018). Rekam kesehatan elektronik (EHR) telah menjadi semakin populer dalam sistem perawatan kesehatan di seluruh dunia. EHR menawarkan banyak manfaat, seperti pengurangan biaya layanan kesehatan, peningkatan akses ke data layanan kesehatan, perawatan mandiri,

kualitas perawatan, dan hasil yang berpusat pada kesehatan dan pasien (Tapuria dkk., 2021). Namun, memastikan keamanan dan privasi data, mengatasi tantangan yang terkait dengan menghubungkan sistem yang beragam, dan memelihara infrastruktur untuk penggunaan data berkualitas tinggi secara berulang-ulang adalah beberapa tantangan yang terkait dengan penggunaan EHR dalam penelitian klinis (Cowie et al., 2017). Di Indonesia, penggunaan Teknologi Informasi dan Komunikasi (TIK) dalam pelayanan kesehatan bertujuan untuk meningkatkan akses, efisiensi, efektivitas, dan kualitas proses medis yang melibatkan organisasi pelayanan medis di rumah sakit, klinik, puskesmas, praktisi medis baik dokter maupun terapis, laboratorium, apotek, asuransi dan melibatkan pasien sebagai konsumen. Namun, proses pelayanan dengan menggunakan program E-health akan mengumpulkan beberapa data pribadi konsumen yang merupakan data pribadi yang bersifat sensitif dan menimbulkan permasalahan hukum baru, yaitu sejauh mana penyelenggara pelayanan kesehatan dapat melindungi data pribadi pasien yang dapat diakses, disebarluaskan dengan lebih mudah melalui kemajuan TIK (Hutabarat dkk., 2022). Hingga saat ini, Indonesia belum memiliki satupun undang-undang yang secara khusus mengatur tentang perlindungan data pribadi. Kondisi ini menyebabkan kasus kebocoran data pribadi pasien masih sering terjadi (Kharisma & Diakanza, 2022). Namun, pada tahun 2022 Republik Indonesia mengesahkan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Sementara di Singapura, Malaysia, Filipina, dan pada tingkat yang lebih rendah, Indonesia dan Vietnam, undang-undang privasi data telah diberlakukan. Namun, hanya ada sedikit kemajuan sejak tahun 2014 di lima anggota lainnya (Brunei, Kamboja, Laos, Myanmar, dan Thailand), sehingga secara keseluruhan, hanya ada sedikit kemajuan menuju 'koherensi' yang menjadi tujuan Masyarakat Ekonomi ASEAN (MEA) (Greenleaf, 2017). Untuk mengatasi tantangan ini, para peneliti telah mengusulkan berbagai solusi, seperti analisis data pasien yang menjaga privasi, pembelajaran federasi, dan komputasi multi-partai (Mantas, 2022; Zhang dkk., 2022). Selain itu, privasi berdasarkan desain dan minimalisasi dalam catatan kesehatan elektronik kecil telah diusulkan sebagai solusi untuk memastikan privasi dan keamanan data (Conte dkk., 2022). Kesimpulannya, perlindungan hukum sangat penting dalam menjaga privasi data pasien dalam sistem kesehatan elektronik. Negara-negara perlu

memberlakukan undang-undang dan peraturan yang secara khusus membahas perlindungan data pribadi untuk memastikan bahwa data pribadi dan medis pasien dijaga kerahasiaan dan keamanannya. Para peneliti dan penyedia layanan kesehatan juga perlu terus mengembangkan dan menerapkan solusi yang menjaga privasi untuk mengatasi tantangan yang terkait dengan penggunaan EHR dalam penelitian klinis.

SIMPULAN

Studi ini membandingkan regulasi dan perlindungan hukum terhadap privasi data pasien dalam sistem kesehatan elektronik di Indonesia, Singapura, dan Laos. Laporan ini memaparkan informasi tentang kerangka kerja legislatif masing-masing negara, otoritas perlindungan data, metode persetujuan, langkah-langkah keamanan data, peraturan transfer data lintas batas, dan perlindungan hukum bagi pasien. Temuan-temuannya menunjukkan kekuatan dan keterbatasan kerangka kerja peraturan di ketiga negara tersebut. Undang-Undang Perlindungan Data Pribadi (PDPA) Singapura terkenal karena pendekatannya yang komprehensif, mekanisme penegakan hukum yang kuat, dan peraturan pemberitahuan pelanggaran data. Meskipun Indonesia dan Laos telah melakukan upaya untuk mengatur privasi data pasien, masih ada kebutuhan untuk perbaikan, seperti mekanisme penegakan hukum yang lebih baik, persyaratan eksplisit untuk notifikasi pelanggaran data, dan harmonisasi dengan standar internasional.

Tantangan yang teridentifikasi termasuk keterbatasan sumber daya, kesenjangan kesadaran dan kepatuhan, risiko keamanan siber, dan pembagian data lintas batas. Tantangan-tantangan ini membutuhkan upaya bersama dari para pembuat kebijakan, organisasi perawatan kesehatan, dan pemangku kepentingan untuk mengatasinya secara efektif. Untuk meningkatkan perlindungan privasi data pasien, beberapa arahan di masa depan direkomendasikan. Memperkuat mekanisme penegakan hukum, meningkatkan kolaborasi internasional untuk menyelaraskan standar perlindungan data, mempromosikan tata kelola dan akuntabilitas data, meningkatkan kesadaran publik dan memberdayakan pasien, serta terus mengevaluasi dan mengadaptasi kerangka kerja peraturan adalah langkah-langkah penting. Para pembuat kebijakan perlu mengalokasikan sumber daya yang cukup dan membangun mekanisme penegakan hukum yang

kuat untuk memastikan kepatuhan terhadap peraturan privasi data pasien. Kolaborasi antar negara dapat memfasilitasi harmonisasi standar perlindungan data dan memfasilitasi transfer data lintas batas yang aman. Organisasi perawatan kesehatan harus memprioritaskan tata kelola data, menerapkan prinsip-prinsip privasi sesuai desain, dan membangun struktur akuntabilitas untuk melindungi data pasien secara efektif. Meningkatkan kesadaran publik tentang hak privasi data pasien dan memberdayakan individu untuk melakukan kontrol atas informasi kesehatan mereka adalah penting. Kampanye edukasi dapat membantu pasien memahami hak-hak mereka, pentingnya persetujuan, dan cara melindungi data mereka. Transparansi dan kepercayaan antara penyedia layanan kesehatan dan pasien sangat penting untuk menjaga privasi data.

DAFTAR PUSTAKA

- Asija, R., & Nallusamy, R. (2014). Data model to enhance the security and privacy of healthcare data. *2014 IEEE Global Humanitarian Technology Conference - South Asia Satellite, GHTC-SAS 2014*, 237–244. <https://doi.org/10.1109/GHTC-SAS.2014.6967590>
- Conte, R., Sansone, F., Tonacci, A., & Pala, A. P. (2022). Privacy-by-Design and Minimization within a Small Electronic Health Record: The Health360 Case Study. *Applied Sciences (Switzerland)*, 12(17). <https://doi.org/10.3390/app12178441>
- Cowie, M. R., Blomster, J. I., Curtis, L. H., Duclaux, S., Ford, I., Fritz, F., Goldman, S., Janmohamed, S., Kreuzer, J., Leenay, M., Michel, A., Ong, S., Pell, J. P., Southworth, M. R., Stough, W. G., Thoenes, M., Zannad, F., & Zalewski, A. (2017). Electronic health records to facilitate clinical research. *Clinical Research in Cardiology*, 106(1), 1–9. <https://doi.org/10.1007/s00392-016-1025-6>
- Dumitrescu, R.-M. (2018). Processing of personal and medical data by judicial institutions in the context of the enforcement of Regulation EU 2016/679—General Data Protection Regulation (GDPR). *Journal of Comparative Research in Anthropology and Sociology*, 9(01), 1–18.
- Eckhoff, D., & Wagner, I. (2017). Privacy in the smart city—applications, technologies, challenges, and solutions. *IEEE Communications Surveys & Tutorials*, 20(1),

- 489–516.
- Goddard, M. (2017). Viewpoint: The EU general data protection regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703–706. <https://doi.org/10.2501/IJMR-2017-050>
- Greenleaf, G. (2017). Asean 's Two Speed Data Privacy Laws: Some Race Ahead. *Privacy Laws & Business International Report* 25, 7.
- Greenleaf, G. (2020). 2020 Ends a Decade of 62 New Data Privacy Laws. *Privacy Laws & Business International Report*, 163(January 2019), 24–26. <https://www.bocra.org/bw/data-protection-act>
- Greenleaf, G., & Cottier, B. (2020). Comparing African Data Privacy Laws: International, African and Regional Commitments. *SSRN Electronic Journal*, December 2014, 18–21. <https://doi.org/10.2139/ssrn.3582478>
- Greenleaf, G., Systems, I., & South, N. (2012). ASEAN 's ' new ' data privacy laws : 116, 22–24.
- Harrigan, P., Coussement, K., Lancelot Miltgen, C., & Ranaweera, C. (2020). The future of technology in marketing; utopia or dystopia? *Journal of Marketing Management*, 36(3–4), 211–215. <https://doi.org/10.1080/0267257X.2020.1744382>
- Hutabarat, D. T. H., Zebua, R., Sitorus, R. A., Subakti, F. A., Ramadhani, H., Mangunsong, J., Nduru, F., Alfah, G. S., Pasaribu, J. C. D., Malau, R. M., Anhar, I., & Sahdan, P. (2022). the Urgency of Legal Protection Against the Implementation of Electronic Information Technology-Based Medical Records in Regulation of the Minister of Health of the Republic of Indonesia Number 269 of 2008. *Journal of Humanities, Social Sciences and Business (Jhssb)*, 1(4), 59–68. <https://doi.org/10.55047/jhssb.v1i4.234>
- Intersoft Consulting. (2018). *General Data Protection Regulation (GDPR)*. <https://gdpr-info.eu/>
- Kang, S., Ho, T. T. T., & Lee, N. J. (2021). Comparative Studies on Patient Safety Culture to Strengthen Health Systems Among Southeast Asian Countries. *Frontiers in Public Health*, 8(January). <https://doi.org/10.3389/fpubh.2020.600216>
- Kharisma, D. B., & Diakanza, A. (2022). Patient personal data protection: comparing the health-care regulations in Indonesia, Singapore and the European Union. *International Journal of Human Rights in Healthcare, ahead-of-print*.
- Mantas, J. (2022). An Improved Infrastructure for Privacy-Preserving Analysis of Patient Data. *Advances in Informatics, Management and Technology in Healthcare*, 295, 144.
- Meinert, E., Alturkistani, A., Brindley, D., Knight, P., Wells, G., & De Pennington, N. (2018). Weighing benefits and risks in aspects of security, privacy and adoption of technology in a value-based healthcare system 15 Commerce, Management, Tourism and Services 1503 Business and Management 08 Information and Computing Sciences 0806 Information Sys. *BMC Medical Informatics and Decision Making*, 18(1), 1–4. <https://doi.org/10.1186/s12911-018-0700-0>
- Natamiharja, R., Sabatira, F., Fakhri, M., Davey, O. M., & Anam, H. (2022). Patient Rights During the Covid-19 Pandemic: the Dilemma Between Data Privacy and Transparency in Indonesia. *Age of Human Rights Journal*, 19(19), 121–136. <https://doi.org/10.17561/tahrj.v19.7004>
- Nugraha, R. I., Purnami, C. T., Prasetijo, A. B., & Wulandari, N. (2023). Pengembangan sistem informasi ibu hamil (sibumil-pe) dalam mendeteksi kejadian preeklampsia di kabupaten bangkalan. *Jurnal Ners*, 7, 984–992.
- Rai, B. K. (2022). Patient-Controlled Mechanism Using Pseudonymization Technique for Ensuring the Security and Privacy of Electronic Health Records. *International Journal of Reliable and Quality E-Healthcare*, 11(1), 1–15. <https://doi.org/10.4018/IJRQEH.297076>
- Sagiroglu, S., & Sinanc, D. (2013). Big data: A review. *2013 International Conference on Collaboration Technologies and Systems (CTS)*, 42–47.
- Shrivastava, U., Song, J., Han, B. T., & Dietzman, D. (2021). Do data security measures, privacy regulations, and communication standards impact the interoperability of patient health information? A cross-country investigation. *International Journal of Medical Informatics*, 148(January), 104401. <https://doi.org/10.1016/j.ijmedinf.2021.104401>
- Tapuria, A., Porat, T., Kalra, D., Dsouza, G., Xiaohui, S., & Curcin, V. (2021). Impact of patient access to their electronic health

record: systematic review. *Informatics for Health and Social Care*, 46(2), 192–204. <https://doi.org/10.1080/17538157.2021.1879810>

Teng, L., Liu, D., & Luo, J. (2022). Explicating user negative behavior toward social media: an exploratory examination based on stressor–strain–outcome model. *Cognition, Technology & Work*, 1–12.

William, P., Yogeesh, N., Vimala, S., & Gite, P. (2022). Blockchain Technology for Data Privacy using Contract Mechanism for 5G Networks. *2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*, 461–465.

Yarali, A., Joyce, R., & Dixon, B. (2020). Ethics of Big Data: Privacy, Security and Trust. *Wireless Telecommunications Symposium, 2020-April*. <https://doi.org/10.1109/WTS48268.2020.9198734>

Zhang, L., Zhu, Y., Ren, W., Zhang, Y., & Choo, K.-K. R. (2022). Privacy-preserving fast authentication and key agreement for e-health systems in iot, based on three-factor authentication. *IEEE Transactions on Services Computing*, 01, 1.