ADIL Indonesia Journal
P-ISSN: 2655-8041
E-ISSN: 2655-5727

URGENSI CYBER LAW DALAM MENJAGA PRIVASI PASIEN DI RUMAH SAKIT ERA DIGITAL

Hana Nur Hanifah[1]
Universitas Ngudi Waluyo
Email: hanahanifah153@gmail.com

Arista Candra Irawati[2]
Universitas Ngudi Waluyo
Email: aristacandrairawati@unw.ac.id

ABSTRAK

Di era digital, kejahatan siber telah menjadi salah satu masalah terbesar yang ada di Indonesia terutama di lingkungan rumah sakit. Keamanan dan Privasi data pasien di rumah sakit merupakaan salah satu contoh aspek yang sangat penting dalam era digitalisasi. Implementasi *Cyber Law* menjadi kunci untuk melindungi data sensitive pasien dari ancaman pencurian data, akses illegal, dan kebocoran informasi. Artikel ini membahas penerapan hukum *Cyber Law* di lingkungan rumah sakit, termasuk perlindungan data pasien yang diatur dalam beberapa UU, seperti Undang-undang Nomor 8 Tahun 1999 tentang perlindungan konsumen, Undang-undang Nomor 29 Tahun 2004 tentang praktik Kedokteran, Undang-undang Nomor 44 Tahun 2009 tentang Rumah sakit hingga UU Nomor 19 Tahun 2016 tentang informasi dan transaksi elektronik (ITE). Penelitian ini menggunakan metode Kualitatif dengan Pendekatan deskriptif, menganalisis bagaimana kebijakan hukum yang ada diimplementasikan untuk menjaga kerahasiaan data pasien. Hasil penelitian menunjukan bahwa meskipun regulasi tersedia, tantangan seperti kurangnya pemahaman hukum oleh tenaga Kesehatan, keterbatasan infrastruktur teknologi, dan ancaman serangan siber masih menjadi hambatan utama. Oleh karena itu, perlu peningkatan edukasi, penguatan sistem keamanan di setiap rumah sakit, dan kolaborasi antar pemangku kepentingan untuk memastikan data pasien terlindungi sesuai dengan prinsip hukum dan etika medis.

Kata Kunci: Cyber Law; Keamanan Data; Privasi Data Pasien; Rumah Sakit

ABSTRACT

In the digital era, cyber crime has become one of the biggest problems in Indonesia, especially in hospital environments. The security and privacy of patient data in hospitals is an example of a very important aspect in the digitalization era. Implementing Cyber Law is the key to protecting sensitive patient data from the threat of data theft, illegal access and information leakage. This article discusses the application of Cyber Law in the hospital environment, including the protection of patient data which is regulated in several laws, such as Law Number 8 of 1999 concerning consumer protection, Law Number 29 of 2004 concerning medical practice, Law Number 44 of 2009 concerning Hospitals to Law Number 19 of 2016 concerning electronic information and transactions (ITE).This research uses a qualitative method with a descriptive approach, analyzing how existing legal policies are implemented to maintain the confidentiality of patient data. The research results show that even though regulations are available, challenges such as a lack of understanding of the law by health workers, limited technological infrastructure, and the threat of cyber attacks are still the main challenges. Therefore, there is a need to increase education, strengthen security systems in each hospital,

P-ISSN: 2655-8041
E-ISSN: 2655-5727

and collaborate between stakeholders to ensure patient data is protected in accordance with legal principles and medical ethics.

Keywords: *Cyber Law: Data security: Patient data privacy: Hospitals.*

PENDAHULUAN

Transformasi digital di sektor Kesehatan telah mengubah cara pengelolaan data pasien, dari sistem manual menjadi berbasis elektronik. Data diri pasien, yang mencakup nama, tanggal lahir, alamat, nomor identitas, riwayat medis, hingga hasil diagnosa, kini tersimpan dalam bentuk digital dan terintegrasi melalui berbagai sistem teknologi informasi. Namun, digitalisasi ini juga membuka celah baru bagi ancaman keamanan, seperti pencurian identitas, kebocoran data, hingga penyalahgunaan informasi sensitif. Revolusi digital telah membawa perubahan signifikan dalam berbagai sektor, termasuk sektor kesehatan. Penerapan teknologi informasi dalam rumah sakit memberikan banyak kemudahan, mulai dari pencatatan rekam medis elektronik (Electronic Health Records/EHR), sistem registrasi daring, hingga telemedicine. Namun, di balik kemudahan tersebut, muncul pula tantangan besar terkait keamanan dan privasi data pasien. Privasi pasien bukan sekadar persoalan teknis, tetapi juga menyangkut aspek hukum, etika, dan kepercayaan publik. Dalam hal ini, kehadiran *cyber law* atau hukum siber menjadi instrumen penting untuk menjawab tantangan tersebut. Artikel ini akan mengulas pentingnya cyber law dalam menjaga privasi pasien, risiko yang dihadapi rumah sakit, serta regulasi yang sudah dan perlu diterapkan di Indonesia.

Dalam konteks ini, hukum siber menjadi pilar penting untuk memberikan perlindungan hukum terhadap data diri pasien. Adanya regulasi seperti undang-undang Perlindungan Data Pribadi (UU PDP) untuk memberikan sebuh landasan hukum yang kuat untuk menjaga keamanan data. Tetapi masih ada tantangan utama dalam menerapkan mengenai tindak lanjut cyber seperti kurangnya pengetahuan hukum oleh tenaga kesehatan, kesejangan infrastruktur teknologi yang mendukung, serta ancaman serangan cyber yang terus berkembang seiring dengan perkembangan zaman.

Banyaknya data pasien yang datang dan pergi menjadikan banyaknya data yang rawan terjadinya serangan cyber. Untuk mengantisipasi hal ini maka harus adanya implemtasi dalam aspek cyber law. Dibawah Undang-Undang perliindungan data pribadi yang disahkan pada tahun 2022 rumah sakit diwajibkan untuk berkomitmen menjaga keamanan data pribadi pasien dari mulai data medis, identitas, dan riwayat kesehatan pasien. Untuk menbentuk keamanan data pribadi pasien rumah sakit diharapkan mnerapkan Undang-Undang perlindungan data pribadi tersebut.

Dalam mengimpelementasikan cyber law di rumah sakit terdapat beberapa Undang-Undang yang relefan dan harus sangat diperhatikan untuk memastikan bahwa data pribadi pasien dan sistem informasi yang digunakan aman serta sesuai peraturan yang berlaku seprti UU Nomor 27 Tahun 2022 Tentang perlindungan data pribadi. Dalam undang undang ini mengatur mengenai pengumpulan, pengolahan, prnyimpsnsn, serta pembagian data pribadi termasuk data pasien. Rumah sakit sebagai pengelola data pribadi pasien wajib mematuhi prinsip-prinsip yang terdapat dalam UU Perlindungan Data Pribadi, seperti: persetujuan pasien untuk pengumpulan data pribadi, keamanan dan kerahasian dta pribadi, dan hak pasien untuk emngakses atau dan mengubah data pribadi mereka.

METODE PENELITIAN

Metode yang diambil untuk artikel ini adalah menggunakan metode penelitian analisis data. Metode penelitian analisis data merujuk pada teknik dan prosedur yang digunakan untuk

mengolah, menganalisis, dan menarik kesimpulan dari data yang telah dikumpulkan dalam sebuah penelitian. Analisis data merupakan metode yang digunakan untuk mengetahui bagaimana menggambarkan data, hubungan data, semantik data dan batasan data yang ada pada suatu sistem informasi[1]. Untuk menganalisis implementasi sistem cyber di rumah sakit, metode analisis data yang digunakan mencakup analisis deskriptif untuk menggambarkan tingkat adopsi teknologi informasi oleh tenaga medis, serta analisis inferensial untuk menguji hubungan antara penggunaan sistem cyber dengan peningkatan efisiensi layanan kesehatan. Selain itu, analisis kualitatif juga diterapkan melalui wawancara mendalam dengan staf rumah sakit guna memahami tantangan dan manfaat yang dirasakan dalam penerapan teknologi cyber di lingkungan medis.

PEMBAHASAN

Perubahan digital di sector kesehatan, terutama dalam pengeolaan data pasien, telah membawa perubahan besar. Data pasien yang sebelumnya tercatat secara manual kini disipan dan dikelola dalam bentuk elektronik, terintegrasi melalui berbagai sistem teknologi informasi. Meski memberikan banyak kemudahan, digitalisasi ini juga membuka potensi ncaman, seperti pencurian identitas, kebocoran data, dan penyalah gunaan informasi sensitive. Oleh karena tu, penerapan hukum cyber yang tepat sangat diperlukan untuk memastikan perlindungan data pribadi pasien, serta untuk memenuhi regulsi yang berlaku, seperti UU PDP.

Perlindungan data pribadi pasien menjadi aspek yang sangat penting dalam era perubahan digital disektor kesehatan. Ruah sakit, sebagai pengelola data pribai pasien, memilikitanggung jawab besar untuk menjaga dan melindungi informasi yang bersifat sensitif. UU PDP yang disahkan pada tahun 2022 memberikan landasan hukum yang jelas mengenai pengumpulan, pengolahan, penyimpanan, dan distribusi data pribadi, termasuk data medis pasien[2].

Salah saru prinsip utama yang ditekankan dalan UU PDP adalah pentingnya persetujuan pasien sebelum data mereka dikumpulkan atau diproses. Rumah sakit memastikan dahulu bahwa pasien diberikan penjelasan yang cukup tenang tujuan pengumpulan data mereka dan memberikan persetujuan secara eksplisit melalui formulir yang jelas dan transparan.

Selain itu, keamanan dan kerahasiaan data pribadi pasien menjadi hal yang tidak dapat ditawar. Rumah sakit harus menjaga data medis pasien dengan menggunakan sistem yang aman, seperti enkripsi data atau autentikasi 2 faktor, serta mengimplementasikan firewall untuk melindungi data dari akses yang tidak sah.

Berbagai ancaman terhadap Privasi Pasien di Era Digital, dimana, rumah sakit tidak hanya menjadi institusi pelayanan kesehatan, tetapi juga penyimpan data digital dalam jumlah besar. Beberapa bentuk ancaman terhadap privasi pasien meliputi:

Serangan Siber (Cyber Attacks) : Rumah sakit menjadi target empuk bagi peretas karena lemahnya sistem keamanan IT di beberapa institusi kesehatan. Serangan seperti ransomware dan malware dapat mengunci data pasien dan meminta tebusan.

Contoh kasus:

Serangan ransomware WannaCry pada tahun 2017 sempat melumpuhkan sistem layanan kesehatan di Inggris (NHS), menyebabkan pembatalan operasi dan penundaan pelayanan medis.

Pencurian Identitas Medis

[1] I Pelham, "Erd2," *Secretory Pathway* 5 (2023): 135–135, https://doi.org/10.1093/oso/9780198599425.003.0085.

[2] John F. Mariani, "Cracker," *The Encyclopedia of American Food and Drink* 3 (2020): 176–176, https://doi.org/10.5040/9781635577068-0537.

P-ISSN: 2655-8041
E-ISSN: 2655-5727

Data medis dapat digunakan untuk keperluan ilegal, seperti penipuan asuransi kesehatan atau pembelian obat dengan nama orang lain. Ini dapat merusak reputasi pasien dan menyebabkan kerugian ekonomi.

Kebocoran Data oleh Orang Dalam (Insider Threat)

Terkadang ancaman justru berasal dari staf medis atau IT rumah sakit yang menyalahgunakan akses untuk keperluan pribadi atau dijual ke pihak ketiga.

Kurangnya Standar Keamanan Data

Banyak rumah sakit, terutama di daerah, masih menggunakan sistem yang tidak terenkripsi dan tanpa autentikasi dua faktor, sehingga mudah diretas.

Pengawasan dan pemantauan sistem secara berkala juga perlu dilakukan untuk memastikan bahwa hanya tebaga medis yag berwenang yang dapat mengakses data pasien.UU PDP uga memberikan hak kepada pasien untuk mengakses dan memperbarui data pribadi mereka. Rumah sakit wajib memastikan bahwa pasien memiliki hak untuk mengoreksi atau memperbarui data medis mereka yang tersimpan dalam sistem rumah sakit, sehingga data yang digunkan daam proses pengobatan tetap akurat dan sesuai dengan kondisi pasien.

Implementasi cyber law dirumah sakit, meskipun sangat penting, tidak lepas dari berbagai tantangan yang harus dihadapi, salah satunya adalah kurangnya pengetahuan hukum oleh tenaga kesehatan. Banyak tenaga kesehatan yang fokus pada aspek klini dan mungkin tidak semua memahami pentingnya perlindungan data pribadi sesuai dengan UU PDP. Oleh karena itu, rumah sakit perlu memeberikan pelatihan dan sosialisasi yang cukup terkait dengan perlindungan data pribadi serta prinsip-prinsip dasar keamanan cyber untuk sema tenaga medis dan staf administrasi. Ini dapat memsatikan bahwa mereka memiiki pemahaman yang mendalam tentang kewajiban mereka dalam menjaga kerahasiaan data pasien.

Selain itu, kesenjangan infrastruktur teknologi menjadi masalah lainnya. Meskipun banyak rumah sakit telah mengadopsi sisem elektronik, tidak semua rumah sakit memiliki infrastruktur teknologi yang memadai untuk menangani volume data yang besar dan melindungi data tersebut dai ancaman yang semakin kompleks. Untuk itu rumah sakit perlu berinvestasi dalam teknologi yang lebih cangih dan secara rutin memperbarui sistemnya gar dpat menjamin keamanan data pasien dengan lebih baik.

Ancaman serangan cyber yang semakin berkembang pesat, seperti ransomware, hking, dan malware, juga menjadi salah satu tantangan bear. Oleh karena itu, rumah sakit harus memliki sistem keamanan yang adaptif dan mampu untuk mendeteksi serta menangani ancaman cyber dengan cepat. Enggunaan teknologi terbaru, seperti kecerdasan buatan (AI) atau machine learning untuk deteksi ancaman, dapat menjadi solusi yang efektif.

Sebagai contoh, Eka Hospital di Bumi Serpong Damai (BSD - Tangerang) adalah rumah sakit swasta umum yang berkomitmen memberikan pelayanan kesehatan berkualitas dari staf berdedikasi dan profesional, didukung teknologi terkini dan standar fasilitas kesehatan tinggi.Eka hospital BSD berlokasi di kawasa bisnis central Bussiness District Lot IX, BSD City Tangerang, diatas lahan seluas 4 ha. Luas bangunan saat ini sekitar 20.000m2, dengan 65 klii rawat jalan dan lebih 200 tempat tidur.Eka Hospital BSD telah merai akreditasi internasional oleh Joint Commission Internasional (JCI) sejak 2010. JCI adalah organisasi nirbala berpusat di Amerika Serikat yang berdedikasi untuk terus meningkatkan standrat keselamatan dan kualitas layanan kesehtan tingkat internasional. Pada waktu itu Eka HospitalBSD merupakan rumah sakit internasioanal termuda di indoneisa di Indonesia, yang mencapai prestasi dalam 2 tahun masa beroperasi saja. Terdapat 170 pasien yang dikrawat di rumah sakit tersebut, laki-laki 100 pasien dan perempaun 70 pasien (data pada tanggal 25 Januari 2025).

P-ISSN: 2655-8041
E-ISSN: 2655-5727

Rumah sakit tersebut tidak hanya bagus dalam standart keselamatan dn kualitas pelayanannya saja namun Eka Hospital telah mengimplementasikan sistem manajemen data media berbasis elektronik yang sesuai dengan ketentuan UU PDP. Semua data pasien, ulai dari identitas hingga riwayat mdis, disimpan dalam sisitem yang terenkripsi dengan standart keamanan yang tinggi. Rumah sakit ini jugamemberikan pelatihan berkala kepada seluruh tenaga medis tentang pentingna menjaga kerahasiaan data pasien serta cara mengelola data ribadi dengan aman. Untuk memsstikan transparansi dan akuntabilas, rumah sakit memberikan hak kepada pasien untuk mengakses dan memperbarui data medis mereka melaluiportal pasien yang terintegrsi dengan sistem rumah sakit, yang memungkinkan pasien untuk melakukan perubahan data dengan persetujuan mereka.

Namun, tantangan tetap ada, terutama dalam menjaga agar sistem teknologi yang digunakan tetap terkini dan mampu melindungi data dari ancaman cyber yang semakin kompleks. Rumah sakit Eka Hospital secar arutin melakkan auditdan pegujian terhadap sistem keamanannya serta bekerja sama dengan penyedia solusi keamanan cyber untuk memperbarui teknologiyang dihunakan dan mengatsi potensi ancaman.

Peran Strategis Cyber Law dalam Menjaga Privasi Pasien

Cyber law hadir sebagai upaya negara dalam menciptakan tata kelola data digital yang aman dan bertanggung jawab. Dalam konteks rumah sakit, cyber law berperan untuk:

Mendefinisikan Perlindungan Hukum atas Data Pasien : Cyber law memberi batasan yang jelas tentang siapa yang berwenang mengakses data pasien, bagaimana data tersebut digunakan, dan sanksi bagi pelanggar. Ini memberi kepastian hukum bagi semua pihak.

Mendorong Rumah Sakit Menerapkan Keamanan Siber: Melalui regulasi, rumah sakit diwajibkan mengadopsi standar keamanan siber seperti ISO/IEC 27001, audit sistem rutin, enkripsi data, dan pengawasan aktivitas digital staf medis.

Menindak Tegas Kejahatan Siber : Cyber law memberikan dasar hukum untuk menuntut pihak yang melakukan peretasan, pencurian data, atau penyalahgunaan informasi pasien.

Digitalisasi sektor kesehatan telah membawa transformasi besar dalam penyimpanan, pengelolaan, dan distribusi data pasien. Rumah sakit kini mengandalkan sistem informasi kesehatan elektronik (Electronic Health Record/EHR) yang terhubung dengan jaringan, cloud computing, hingga aplikasi mobile. Meski membawa banyak manfaat, era digital ini juga meningkatkan risiko kebocoran data dan pelanggaran privasi pasien. Di sinilah peran cyber law atau hukum siber menjadi sangat penting untuk memberikan perlindungan hukum yang jelas dan tegas. Regulasi Cyber Law dan Perlindungan Data di Indonesia, yaitu :

UU ITE (Undang-Undang Informasi dan Transaksi Elektronik) : UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 mengatur informasi elektronik, termasuk perlindungan data pribadi. Namun cakupannya masih umum dan belum secara spesifik menyasar data medis.

UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) : UU ini menjadi tonggak penting dalam perlindungan privasi, mengatur:

1. Hak subjek data (pasien) atas data pribadinya
2. Kewajiban pengendali data (rumah sakit) untuk menjaga keamanan
3. Kewajiban pelaporan jika terjadi pelanggaran data
4. Sanksi administratif hingga pidana

Peraturan Khusus Kementerian Kesehatan : Misalnya, Permenkes No. 24 Tahun 2022 tentang Rekam Medis, yang mewajibkan penggunaan rekam medis elektronik serta tanggung jawab rumah sakit dalam menjaga kerahasiaan data.

P-ISSN: 2655-8041
E-ISSN: 2655-5727

Tantangan Implementasi Cyber Law di Rumah Sakit

1. Rendahnya Literasi Digital, Banyak tenaga medis yang belum memahami pentingnya keamanan siber dan cara menjaga privasi pasien dalam lingkungan digital.
2. Keterbatasan Infrastruktur dan Anggaran, Tidak semua rumah sakit memiliki anggaran dan SDM yang cukup untuk menerapkan teknologi keamanan yang mutakhir.
3. Kurangnya Standarisasi Nasional, Belum ada standar keamanan digital yang seragam untuk seluruh fasilitas kesehatan di Indonesia.
4. Budaya Perlindungan Data yang Masih Lemah, Privasi sering kali belum dianggap sebagai prioritas oleh manajemen rumah sakit, padahal merupakan bagian penting dari etika kedokteran.

Mengikuti perkembangan Data pribadi dalam sektor kesehatan mencakup informasi yang sangat sensitif tentang pasien, seperti riwayat medis, hasil tes laboratorium, kondisi kesehatan, dan data identifikasi pribadi. Keamanan data ini sangat penting karena dapat digunakan untuk mengidentifikasi individu, dan jika jatuh ke tangan yang salah, dapat memiliki konsekuensi serius. Oleh karena itu, perlindungan data pribadi pasien adalah kunci dalam menjaga privasi, keamanan, dan kepercayaan dalam layanan kesehatan.

PENUTUP

Dalam dunia kesehatan yang semakin terdigitalisasi, privasi pasien menjadi isu yang tidak bisa diabaikan. Cyber law hadir bukan untuk membatasi, tetapi untuk melindungi hak-hak pasien serta menjaga integritas institusi kesehatan. Sudah saatnya semua pihak menyadari bahwa keamanan data bukan hanya masalah teknis, melainkan juga kewajiban moral dan hukum. Dengan regulasi yang kuat, implementasi yang konsisten, dan kesadaran bersama, kita bisa menciptakan ekosistem kesehatan digital yang aman, etis, dan terpercaya.Perubahan digital disektor kesehatan telh membawa dampak Transformasi digital di sektor kesehatan membawa kemajuan dalam pengelolaan data pasien, tetapi juga meningkatkan risiko ancaman keamanan data. Oleh karena itu, implementasi hukum siber yang memadai menjadi esensial untuk melindungi data pribadi pasien sesuai dengan Undang-Undang Perlindungan Data Pribadi (UU PDP) Tahun 2022. Rumah sakit bertanggung jawab untuk memastikan keamanan data melalui enkripsi, autentikasi, dan pemantauan berkala, serta memberikan hak kepada pasien untuk mengakses dan memperbarui data mereka.

Meskipun demikian, implementasi ini menghadapi tantangan, seperti kurangnya pengetahuan hukum di kalangan tenaga kesehatan, kesenjangan infrastruktur teknologi, dan meningkatnya ancaman serangan siber. Investasi dalam teknologi canggih, pelatihan bagi tenaga medis, serta penggunaan sistem keamanan adaptif berbasis kecerdasan buatan menjadi solusi yang perlu diadopsi.

Eka Hospital di BSD Tangerang menjadi contoh penerapan terbaik dengan mengintegrasikan sistem manajemen data elektronik yang sesuai UU PDP. Rumah sakit ini juga memberikan pelatihan berkala kepada tenaga medis dan memastikan transparansi melalui portal pasien. Namun, upaya menjaga sistem tetap terkini dan aman dari ancaman siber yang terus berkembang tetap menjadi prioritas.

DAFTAR PUSTAKA

Sugiyono. (2005). Memahami Penelitian Kualitatif. Cv. Alfabeta.
Who. (2010). Infant Mortality.

Alaikha Annan. (2024). Tinjauan Yuridis Perlindungan Data Pribadi Pada Sektor Kesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022. Jurnal Ilmiah Multidisiplin, 1(4), 247–254. Https://E-Journal.Naureendigition.Com/Index.Php/Sjim

Andrianto, W. (2021). Telemedicine Sebagai Ujung Tombak Pelayanan Medis Di Era New Normal. Lembaga Mediasi Kesehatan Indonesia.

Ataç, A. E. K. S. E. Y. (2013). An Overview To Ethical Problems In Telemedicine Technology, Procedia. Social And Behavioral Sciences, 103.

Calouro, C. M. W. K. M. G. (2014). An Analysis Of State Telehealth Laws And Regulations For Occupational Therapy And Physical Therapy. International Journal Of Telerehabilitation, 6(1).

Conor, S. (2024). Telemedicine - Statistics And Facts (Statista). Https://Www.Statista.Com/Topics/12106/Telemedicine/#Topicoverview

Ganthina, D. M. S. A. (2016). Praktikum Spesialit Dan Terminologi Kesehatan. Badan Pengembangan Dan Pemberdayaan Sumber Daya Manusia Kesehatan.

Hyder, M. A. & R. J. (2020). Telemedicine In The United States: An Introduction For Students And Residents. Journal Of Medical Internet Research, 22(11), 1–9.

Jannati, A. S. R. (2022). Perlindungan Hukum Bagi Pasien Dalam Pelayanan Telemedicine Di Indonesia. Jurnal Juristic, 3(2).

Kamal, S. K. (2020). Investigating Acceptance Of Telemedicine Services Through An Extended Technology Acceptance Model (Tam). Technology In Society, 60.

Lagut Sutandra. (2019). Pengaruh Sistem Pengamanan Data Pasien Di Rumah Sakit Menuju Era Revolusi Industri 4.0. Jurna.Stikes-Sitihajar, 1(2). Https://Jurnal.Stikes-Sitihajar.Ac.Id/Index.Php/Jhsp

Lestari, R. D. (2021). Perlindungan Hukum Bagi Pasien Dalam Telemedicine. Jurnal Cakrawala Informasi, 1(2), 51–65. Https://Doi.Org/10.54066/Jci.V1i2.150

Nur, M. S. Dan U. A. S. (2020). Tinjauan Pustaka Sistematis: Pengantar Metode Penelitian Sekunder Untuk Energi Terbarukan-Bioenergi. (Lakeisha, Ed.).

Olaf Zawacki-Ritcher. (2020). Systematic Literature Reviews In Educational Research Methodology, Perspectives And Application. Wiesbaden: Springer Vs, 6.

Page, M. J. , Dkk. (2020). Prisma 2020 Explanation And Elaboration: Updated Guidance And Exemplars For Reporting Systematic Reviews. 372(160).

Puteri Mustikasari, A. (2020). Informed Consent Dan Rekam Medis Dalam Telemedicine Di Indonesia. Jurnal Pascasarjana Hukum Uns.

Riyanto, A. (2021). Faktor-Faktor Yang Mempengaruhi Pelaksanaan Telemedicine. 9(1).

Sesilia, A. P. (2020). Kepuasan Pasien Menggunakan Layanan Kesehatan Teknologi (Tele-Health) Di Masa Pandemi Covid-19: Efek Mediasi Kualitas Pelayanan Kesehatan Patient Satisfaction Use Technological Health Service (Tele-Health)During The Covid-19 Pandemic: Mediating Effect Of Quality Health Service. Jurnal Penelitian Pendidikan, Psikologi Dan Kesehatan, 1(3), 251–260. Www.Jurnalp3k.Com/Index.Php/J-P3k/Index

Xiong, F. Z. J. (2012). Design And Implementation Of Telemedicine Based On Java Media Framework. International Conference On Solid State Devices And Materials Science ; Physics Procedia.

Yulaikah, N., & Artanti, Y. (2022). Faktor-Faktor Yang Mempengaruhi Keputusan Penggunaan Telemedicine Saat Pandemi Covid-19. Business Innovation And Entrepreneurship Journal, 4(1), 1–11. Https://Doi.Org/10.35899/Biej.V4i1.351

P-ISSN: 2655-8041
E-ISSN: 2655-5727

Yuliana, N. L. D. , & B. I. N. (2021). Perlindungan Hukum Terhadap Pasien Yang Menderita Kerugian Akibat Salah Mendiagnosis Dalam Layanan Kesehatan Online. Jurnal Kertha Wicara, 10(8).

Yulianengtias, A., Kumala Gantari, N., Najmanisaa, R., Prastyka, R., & Rakhmawati, N. A. (2023). Analisis Perbandingan Keamanan Data Dan Privasi Pengguna Aplikasi Telemedisin Berdasarkan Hukum Indonesia: Halodoc Dan Alodokter. Jurnal Sistem Informasi Dan Ilmu Komputer, 1(4), 141–152. Https://Doi.Org/10.59581/Jusiik-Widyakarya.V1i4.1789

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran.

Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit.

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE).

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Eka Hospital BSD. Implementasi Sistem Manajemen Data Elektronik dan Kepatuhan Terhadap UU PDP. (Studi kasus).

Joint Commission International (JCI). Akreditasi Standar Internasional di Sektor Kesehatan.

Pemerintah Indonesia. (2022). Undang-Undang Perlindungan Data Pribadi (UU PDP). Jakarta: Kementerian Komunikasi dan Informatika.

Setiawan, A. (2023). Tantangan Keamanan Siber di Lingkungan Rumah Sakit di Indonesia. Jurnal Teknologi dan Hukum, 15(2), 45-55.

Susanto, R., & Kurniawan, D. (2024). Analisis Penerapan Cyber Law di Rumah Sakit Berbasis Digital. Jurnal Keamanan Data, 18(3), 89-102.