



Cyber Criminal Law Analysis on Electronic Medical Record Protection (Study at Mitra Medika Premier Hospital Medan)

Analisis Hukum Pidana Cyber terhadap Perlindungan Rekam Medis Elektronik (Studi di Rumah Sakit Mitra Medika Premier Medan)

Esti Budi Rahayu¹⁾; Ismaidar²⁾;
^{1,2,3)} Universitas Pembangunan Panca Budi
Email: ¹⁾ estibudirah@gmail.com

ARTICLE HISTORY

Received [22 Maret 2026]
Revised [28 April 2026]
Accepted [30 April 2026]

KEYWORDS

Pidana Cyber, Perlindungan,
Rekam Medis Elektronik.

This is an open access article
under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license



ABSTRAK

Dalam era digital saat ini, perkembangan teknologi informasi telah merevolusi berbagai aspek kehidupan manusia, termasuk dalam bidang kesehatan. Penggunaan rekam medis elektronik di rumah sakit telah menjadi standar yang umum, memungkinkan penyimpanan data pasien secara lebih efisien dan akses yang lebih cepat bagi tenaga medis. Namun, bersamaan dengan kemajuan ini, muncul pula tantangan hukum, terutama terkait dengan perlindungan data pribadi pasien. Permasalahan yang dibahas mengenai bagaimana implikasi hukum pidana cyber terhadap perlindungan rekam medis elektronik di rumah sakit, bagaimana kendala dan hambatan dalam melindungi rekam medis elektronik di Rumah Sakit Mitra Medika Premier Medan dan bagaimana upaya pencegahan pidana cyber dalam melindungi rekam medis elektronik di Rumah Sakit Mitra Medika Premier Medan. Penelitian yang digunakan yuridis empiris dengan menggunakan metode pengumpulan data melalui studi lapangan (*field research*) dan studi Pustaka (*library research*). Studi Pustaka yakni diperoleh melalui membaca, mempelajari dan mengkaji buku-buku, aturan perundang-undangan, jurnal ataupun data-data yang berupa bahan pustaka sedangkan studi lapangan dilakukan dengan metode wawancara. Beberapa bentuk pelanggaran yang mungkin terjadi dalam pengelolaan rekam medis elektronik di Rumah Sakit Mitra Medika Premier Medan adalah Akses Tidak Sah (*Unauthorized Access*): Ketika login petugas kesehatan yang tidak hadir ditiptikan pada petugas kesehatan lainnya untuk menggantikan pengentrian data dan Pengambilan Data: Data pasien digunakan oleh pihak tidak berwenang misal foto hasil laboratorium. Upaya yang dilakukan Rumah Sakit Mitra Medika Premier Medan dalam melindungi data Kesehatan meliputi: Penguatan Infrastruktur Teknologi: Penerapan firewall, antivirus, dan enkripsi data, Audit Rutin: Memastikan sistem berjalan sesuai standar keamanan, Peningkatan Kesadaran Staf: Pelatihan reguler terkait perlindungan data dan Update/pengembangan sistem teknologi informasi khususnya terkait security data.

ABSTRACT

In today's digital era, the development of information technology has revolutionized various aspects of human life, including in the field of health. The use of electronic medical records in hospitals has become a common standard, allowing for more efficient storage of patient data and faster access for medical personnel. However, along with these advances, there have also been legal challenges, especially related to the protection of patients' personal data. The problems discussed are how the implications of cyber criminal law on the protection of electronic medical records in hospitals, what are the obstacles and obstacles in protecting electronic medical records at Mitra Medika Premier Medan Hospital and how cyber crime prevention efforts in protecting electronic medical records at Mitra Medika Premier Medan Hospital. The research used is empirical juridical using data collection methods through field research and library research. Literature Studies is obtained through reading, studying and studying books, laws and regulations, journals or data in the form of library materials while field studies are carried out by interview method. Some forms of violations that may occur in the management of electronic medical records at Mitra Medika Premier Medan Hospital are Unauthorized Access: When the login of an absent health worker is entrusted to another health worker to replace data entry and Data Collection: Patient data is used by unauthorized parties, for example photos of laboratory results. The efforts made by Mitra Medika Premier Medan Hospital in protecting health data include: Strengthening Technology Infrastructure: Implementing firewalls, antivirus, and data encryption, Routine Audits: Ensuring that the system runs according to security standards, Increasing Staff Awareness: Regular training related to data protection and Update/development of information technology systems, especially related to data security.

PENDAHULUAN

Perkembangan teknologi dan informasi yang pesat telah mengubah berbagai aspek kehidupan termasuk sektor Kesehatan. Salah satu perubahan yang signifikan yaitu kemunculan era big data. Big data adalah Kumpulan data yang sangat besar dan kompleks sehingga sulit untuk diproses menggunakan metode pengolahan data tradisional (Gandomi & Haider, 2015). Dibidang Kesehatan big data berarti mengumpulkan dan menganalisis informasi medis dalam skala yang belum pernah ada

sebelumnya. Hal ini termasuk data Kesehatan pribadi yang merupakan sumber informasi terpenting tentang status Kesehatan seseorang dalam pelayanan Kesehatan (Raghupathi & Raghupathi, 2014).

Era big data telah membawa perubahan yang signifikan dalam berbagai aspek kehidupan termasuk dalam bidang Kesehatan. Pengumpulan, pengolahan dan analisis data Kesehatan dalam skala besar memiliki potensi untuk menghasilkan pengetahuan baru dan inovasi dalam pelayanan Kesehatan. Namun penggunaan data Kesehatan pribadi dalam era big data menimbulkan berbagai tantangan hukum dan kebijakan (Meher & Irsyam, 2023).

Berkaitan dengan hal tersebut seperti adanya pelayanan Kesehatan yang terbagi atas pelayanan Kesehatan Masyarakat dan pelayanan secara individu. Dalam hubungan ini dokter adalah orang yang dibutuhkan dan dipercaya untuk membantu dalam memberikan dan mengupayakan pengobatan kepada pasien yang sedang membutuhkan suatu penanganan medis. Hubungan antara dokter dan pasien dalam pemberian pelayanan Kesehatan secara individu dimulai pada saat pertama kali seorang pasien datang keruangan praktik dengan membawa keluhan akan kesehatannya. Selanjutnya seorang dokter akan melakukan serangkaian pemeriksaan awal berupa wawancara yang disebut dengan anamnesa yang kemudian akan dilakukan pemeriksaan fisik yang menuju pada sebuah diagnosa pasien. Hasil diagnosa tersebut yang menentukan (Sidi & Ronnie, 2022).

Dalam era digital saat ini, perkembangan teknologi informasi telah merevolusi berbagai aspek kehidupan manusia, termasuk dalam bidang kesehatan. Penggunaan rekam medis elektronik di rumah sakit telah menjadi standar yang umum, memungkinkan penyimpanan data pasien secara lebih efisien dan akses yang lebih cepat bagi tenaga medis. Namun, bersamaan dengan kemajuan ini, muncul pula tantangan hukum, terutama terkait dengan perlindungan data pribadi pasien.

Berdasarkan penjelasan yang terdapat dalam Undang-undang Nomor 17 Tahun 2023 tentang Kesehatan pada penjelasan Pasal 173 Huruf c, bahwa yang dimaksud dengan rekam medis yaitu dokumen yang berisikan data identitas Pasien, Tindakan, pemeriksaan, pengobatan dan pelayanan lain yang telah diberikan kepada pasien yang dibuat dengan menggunakan system elektronik yang diperuntukkan penyelenggaraan rekam medis. Dalam hal fasilitas pelayanan Kesehatan tidak dapat menyelenggarakan rekam medis secara elektronik karena hambatan teknis, dapat digunakan rekam medis non elektronik sampai dengan hambatan selesai serta dilakukan penginputan ulang data rekam medis pada system rekam medis elektronik.

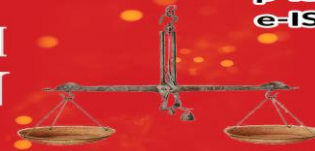
Implikasi hukum pidana *cyber* terhadap perlindungan rekam medis elektronik di rumah sakit menjadi semakin penting. Ancaman keamanan data elektronik, seperti pencurian identitas dan pelanggaran privasi, merupakan masalah yang harus diatasi dengan serius. Hukum pidana *cyber*, yang mencakup aturan dan sanksi terkait kejahatan yang dilakukan melalui jaringan internet, menjadi instrumen penting dalam melindungi integritas dan kerahasiaan rekam medis elektronik.

Hukum pidana *cyber* memiliki peran krusial dalam menegakkan perlindungan data pribadi, termasuk rekam medis elektronik di rumah sakit. Dengan adanya sanksi pidana bagi pelaku yang melakukan akses ilegal atau penyalahgunaan data medis elektronik, diharapkan dapat memberikan *deterrence* yang cukup untuk mencegah kejahatan *cyber* di sektor kesehatan. Namun demikian, tantangan utama dalam menerapkan hukum pidana *cyber* terhadap perlindungan rekam medis elektronik adalah dalam menentukan yurisdiksi dan pembuktian dalam kasus-kasus pelanggaran. Karena sifat lintas batas internet, seringkali sulit untuk menentukan di mana kejahatan itu sebenarnya terjadi, dan pembuktian elektronik dapat menjadi rumit dan memerlukan keahlian khusus.

Oleh karena itu, langkah-langkah perlu diambil untuk memperkuat kerangka hukum pidana *cyber* yang relevan dengan perlindungan rekam medis elektronik. Hal ini melibatkan kerjasama antara pemerintah, lembaga hukum, rumah sakit, dan pakar teknologi informasi untuk mengembangkan kebijakan yang lebih efektif dalam mencegah dan menangani kejahatan *cyber* di sektor kesehatan. Dengan demikian, perlindungan terhadap data pasien dapat diperkuat, dan kepercayaan masyarakat terhadap sistem kesehatan digital dapat dipertahankan atau bahkan ditingkatkan.

Lebih lanjut pengaturan mengenai rekam medis terdapat didalam Undang-undang Nomor 17 Tahun 2023 tentang Kesehatan pada Pasal 296. Penyelenggaraan rekam medis merupakan tanggungjawab fasilitas pelayanan Kesehatan. Setiap tenaga medis dan tenaga Kesehatan yang memberikan pelayanan Kesehatan perseorangan wajib membuat rekam medis. Rekam medis harus segera dilengkapi setelah pasien selesai menerima pelayanan Kesehatan.

Dalam beberapa tahun terakhir, terjadi peningkatan signifikan dalam penggunaan rekam medis elektronik di rumah sakit. Ini merupakan respons terhadap kemajuan teknologi informasi yang memungkinkan penyimpanan dan pertukaran informasi medis secara digital. Rekam medis elektronik mempercepat akses terhadap informasi pasien, memungkinkan koordinasi perawatan yang lebih baik, dan meningkatkan efisiensi operasional. Namun, bersamaan dengan manfaat ini, muncul pula tantangan baru terkait dengan keamanan dan privasi data pasien.



Dalam konteks perkembangan teknologi informasi dalam bidang kesehatan, ada juga perkembangan yang signifikan dalam *telemedicine* atau layanan kesehatan jarak jauh. Teknologi ini memungkinkan pasien untuk berkonsultasi dengan dokter atau tenaga medis tanpa harus secara fisik hadir di rumah sakit. Meskipun memberikan kemudahan aksesibilitas yang besar, *telemedicine* juga menimbulkan pertanyaan hukum terkait dengan privasi dan keamanan data pasien.

Pengaturan penggunaan data Kesehatan pribadi di Indonesia masih menghadapi berbagai tantangan. Salah satunya yaitu belum adanya Undang-undang Perlindungan Data Pribadi yang komprehensif tentang Kesehatan (Nurfadzilah, 2021). Meskipun saat ini terdapat beberapa peraturan yang mengatur penggunaan data pribadi sebagaimana yang terdapat dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-undang Nomor 17 Tahun 2023 tentang Kesehatan. Perlindungan privasi dan keamanan data Kesehatan pribadi belum diatur secara menyeluruh dan Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang ada belum begitu maksimal dijalankan.

Perlunya regulasi yang lebih ketat *dalam* mengatur penggunaan dan penyimpanan data pasien dalam konteks *telemedicine*. Hukum pidana *cyber* juga dapat diterapkan dalam kasus-kasus pelanggaran keamanan data pasien yang terjadi dalam praktik *telemedicine*. Namun, implementasi hukum pidana *cyber* dalam konteks kesehatan juga harus memperhatikan aspek-aspek etis dan praktisnya. Misalnya, dalam menangani pelanggaran keamanan data, penting untuk mempertimbangkan kepentingan kesehatan pasien dan kemungkinan dampak negatif dari pemberian sanksi pidana terhadap institusi kesehatan yang bersangkutan. Oleh karena itu, pendekatan yang seimbang antara penegakan hukum dan kepentingan kesehatan publik perlu diambil dalam menghadapi tantangan ini.

Selain itu, penting juga untuk terus mengembangkan keahlian dan kapasitas dalam bidang hukum pidana *cyber* di kalangan tenaga hukum dan penegak hukum. Pelatihan dan pendidikan yang khusus dalam aspek-aspek hukum yang berkaitan dengan teknologi informasi dan kesehatan akan membantu meningkatkan efektivitas penanganan kasus-kasus pelanggaran data medis elektronik. Implikasi hukum pidana *cyber* terhadap perlindungan rekam medis elektronik di rumah sakit menjadi semakin relevan. Ancaman keamanan *cyber* seperti pencurian data dan serangan *ransomware* dapat mengakibatkan kerugian besar, baik bagi pasien maupun penyedia layanan kesehatan.

Dokumen rekam medis sebagaimana yang terdapat pada Pasal 296 Undang-undang Nomor 17 Tahun 2023 tentang Kesehatan merupakan milik fasilitas pelayanan Kesehatan. Setiap pasien berhak untuk mengakses informasi yang terdapat dalam dokumen rekam medis dan fasilitas pelayanan Kesehatan wajib menjaga keamanan, keutuhan, kerahasiaan dan ketersediaan data yang terdapat dalam dokumen rekam medis.

Salah satu tantangan utama dalam melindungi rekam medis elektronik adalah keamanan sistem informasi yang digunakan untuk menyimpan dan mengakses data tersebut. Diperlukan langkah-langkah teknis yang kuat, seperti enkripsi data dan penggunaan sistem keamanan yang canggih, untuk melindungi informasi medis dari akses yang tidak sah. Selain itu, kepatuhan terhadap regulasi dan standar keamanan data yang berlaku juga penting untuk mengurangi risiko pelanggaran.

Efektivitas penegakan hukum pidana *cyber* terhadap pelanggaran keamanan data medis tergantung pada kerjasama antara lembaga penegak hukum, penyedia layanan kesehatan, dan pihak terkait lainnya. Komunikasi yang baik dan pertukaran informasi yang cepat dapat membantu dalam mendeteksi dan menangani pelanggaran dengan lebih efisien. Namun, dalam menangani kasus-kasus pelanggaran keamanan data medis, perlu juga memperhatikan prinsip-prinsip hak asasi manusia dan privasi. Sanksi pidana harus diberikan dengan proporsionalitas dan memperhitungkan kepentingan kesehatan publik serta hak-hak individu.

Penyelenggaraan Pembangunan Kesehatan meliputi Upaya Kesehatan dan sumber dayanya harus dilakukan secara terpadu dan berkesinambungan diberbagai bidang dan kemajuan ilmu pengetahuan dan teknologi telah meingkatkan taraf kesejahteraan Masyarakat kesadaran akan hidup sehat. Hal ini mempengaruhi meningkatnya kebutuhan pelayanan dan pemerataan yang mencakup tenagam sarana dan prasarana baik jumlah maupun mutu. Oleh karena itu diperlukan pengaturan untuk melindungi pemberi dan penerima jasa pelayanan Kesehatan (Darmawan, et.al, 2023).

Dalam menghadapi kompleksitas tantangan keamanan data medis elektronik, kerjasama lintas sektor antara pemerintah, lembaga kesehatan, dan pelaku industri teknologi informasi menjadi kunci. Langkah-langkah preventif seperti pelatihan keamanan *cyber* bagi staf medis dan pembaruan rutin terhadap sistem informasi akan membantu mengurangi risiko pelanggaran. Dengan demikian, perlindungan terhadap rekam medis elektronik dapat ditingkatkan, dan kepercayaan masyarakat terhadap sistem kesehatan digital dapat dipertahankan.

LANDASAN TEORI

Hukum Pidana Cyber

Hukum pidana *cyber* adalah cabang hukum yang berkaitan dengan kejahatan yang dilakukan melalui atau terhadap sistem komputer dan jaringan internet. Istilah "*cybercrime*" atau "kejahatan *cyber*" mencakup berbagai tindakan yang melanggar hukum yang melibatkan penggunaan teknologi informasi dan komunikasi. Dalam konteks ini, hukum pidana *cyber* mencakup pengaturan dan penegakan hukum terkait dengan akses ilegal ke sistem komputer, penipuan online, pencurian identitas, penyebaran *malware*, dan berbagai kegiatan kriminal lainnya yang terjadi dalam ranah digital.

Hukum Siber (*Cyber Law*) adalah istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Istilah lain yang juga digunakan adalah hukum Teknologi Informasi (*Law of Information Technology*), Hukum Dunia Maya (*Virtual World Law*) dan Hukum Mayantara. Istilah-istilah tersebut lahir mengingat kegiatan internet dan pemanfaatan teknologi informasi berbasis virtual. Istilah hukum siber jika diidentikan dengan "dunia maya" akan cukup menghadapi persoalan ketika terkait dengan pembuktian dan penegakan hukumnya. Mengingat para penegak hukum akan menghadapi kesulitan jika harus membuktikan suatu persoalan yang diasumsikan sebagai "maya", sesuatu yang tidak terlihat dan semu (Ramli, 2006).

Cyber law sendiri adalah hukum yang khusus berlaku di dunia *cyber*. Secara luas *cyber law* bukan hanya meliputi tindak kejahatan di internet, namun juga aturan yang melindungi para pelaku *e-commerce*, *e-learning*, pemegang hak cipta, rahasia dagang, paten, *e-signature* dan masih banyak lagi. *Cyber law* erat lekatnya dengan dunia kejahatan. Hal ini juga didukung oleh globalisasi. Zaman terus berubah-ubah dan manusia mengikuti perubahan zaman. Perubahan itu diikuti oleh dampak positif dan dampak negatif. Ada dua unsur terpenting dalam globalisasi. Pertama, dengan globalisasi manusia dipengaruhi dan kedua, dengan globalisasi manusia saling mempengaruhi (Sulaiman, 2002).

Hukum pidana *cyber* juga dapat diartikan sebagai seperangkat peraturan hukum yang mengatur dan menetapkan tindakan kriminal serta sanksi yang berlaku dalam konteks penggunaan teknologi informasi dan komunikasi. Dalam hal ini, hukum pidana *cyber* bertujuan untuk melindungi keamanan dan integritas sistem informasi serta menghukum pelaku kejahatan yang melakukan penyalahgunaan teknologi tersebut. Pengertian hukum pidana *cyber* juga mencakup upaya pencegahan dan penegakan hukum terhadap tindakan kriminal yang terkait dengan komputer dan jaringan internet.

Hukum pidana *cyber* menempati posisi penting dalam mengatasi ancaman keamanan *cyber* yang semakin kompleks dan meresahkan. Dalam upaya melindungi masyarakat dari kejahatan digital, hukum pidana *cyber* menetapkan aturan-aturan yang mengatur perilaku kriminal dalam lingkungan online serta sanksi yang diberlakukan terhadap pelaku kejahatan tersebut.

Salah satu karakteristik utama hukum pidana *cyber* adalah sifatnya yang dinamis dan terus berubah seiring dengan perkembangan teknologi. Berbagai tindakan kriminal baru terus muncul sejalan dengan kemajuan teknologi informasi dan komunikasi. Oleh karena itu, sistem hukum harus dapat beradaptasi dengan cepat untuk mengatasi ancaman baru dan menegakkan keadilan dalam ranah digital.

Pentingnya hukum pidana *cyber* semakin terasa dalam era digital ini, di mana masyarakat semakin bergantung pada teknologi informasi dan komunikasi dalam kehidupan sehari-hari. Keamanan *cyber* bukan hanya menjadi tanggung jawab individu atau perusahaan, tetapi juga menjadi tanggung jawab pemerintah dan lembaga hukum untuk menciptakan lingkungan digital yang aman dan dapat dipercaya bagi semua pengguna. Dengan demikian, hukum pidana *cyber* memainkan peran krusial dalam memastikan keadilan dan keamanan dalam ruang digital yang semakin kompleks dan terhubung ini.

Rekam Medis Elektronik

Rekam medis elektronik dapat diartikan sebagai sistem penyimpanan informasi medis pasien dalam bentuk digital yang memungkinkan akses cepat dan efisien oleh tenaga medis yang berwenang. Dalam konteks ini, rekam medis elektronik menggantikan metode tradisional berbasis kertas dengan menyimpan data medis dalam format elektronik yang dapat dengan mudah diakses dan dikelola.

Berdasarkan penjelasan yang terdapat dalam Undang-undang Nomor 17 Tahun 2023 tentang Kesehatan pada penjelasan Pasal 173 Huruf c, bahwa yang dimaksud dengan rekam medis yaitu dokumen yang berisikan data identitas Pasien, Tindakan, pemeriksaan, pengobatan dan pelayanan lain yang telah diberikan kepada pasien yang dibuat dengan menggunakan sistem elektronik yang diperuntukkan penyelenggaraan rekam medis. Dalam hal fasilitas pelayanan Kesehatan tidak dapat menyelenggarakan rekam medis secara elektronik karena hambatan teknis, dapat digunakan rekan



medis non elektronik sampai dengan hambatan selesai serta dilakukan penginputan ulang data rekam medis pada system rekam medis elektronik.

Rekam medis elektronik juga dapat diartikan sebagai upaya untuk meningkatkan kualitas pelayanan kesehatan dengan memanfaatkan teknologi informasi dan komunikasi. Dalam hal ini, rekam medis elektronik bertujuan untuk menyediakan informasi medis yang akurat dan terintegrasi untuk mendukung pengambilan keputusan klinis yang lebih baik.

Selanjutnya, pengertian rekam medis elektronik juga mencakup konsep interoperabilitas, yaitu kemampuan sistem informasi kesehatan untuk berkomunikasi dan bertukar informasi dengan sistem lainnya. Namun, dalam menerapkan rekam medis elektronik, penting untuk memperhatikan aspek privasi dan keamanan data pasien. Perlunya kebijakan dan teknologi yang tepat untuk melindungi kerahasiaan informasi medis pasien dalam lingkungan digital.

Berdasarkan ketentuan pada Pasal 189 huruf h Undang-undang Kesehatan pada bagian penjelasan, yang dimaksud dengan menyelenggarakan rekam medis adalah penyelenggaraan rekam medis yang dilakukan sesuai dengan standar yang secara bertahap diupayakan mencapai standar internasional.

METODE PENELITIAN

Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini yaitu yuridis empiris. Yuridis yaitu mengkaji konsep normatifnya atau peraturan perundang-undangan, sedangkan empiris yakni mengkaji pada kenyataan yang ada berkaitan dengan analisis hukum pidana cyber terhadap perlindungan rekam medis elektronik di Rumah Sakit Mitra Medika Premier Medan. Ditinjau dari perkembangan kehidupan dan perubahan-perubahan transformatif yang cepat maka untuk menata perkembangan dan perubahan hukum positif tidak dapat berfungsi secara efektif. Dari berbagai masalah kehidupan, cabang ilmu sosial dan terutama sosiologi perlu untuk ikut berperan dalam menyelesaikannya kemudian hukum dikonsepsikan secara sosiologis sebagai suatu gejala empiris yang dapat diamati di dalam kehidupan (Syamsudin, 2013).

Metode Pengumpulan Data

Penelitian ini menggunakan metode pengumpulan data yang dilakukan dengan studi lapangan (*field research*) dan studi Pustaka (*library research*). Studi Pustaka yakni diperoleh melalui membaca, mempelajari dan mengkaji buku-buku, aturan perundang-undangan, jurnal ataupun data-data yang berupa bahan Pustaka sedangkan studi lapangan yakni dilakukan dengan metode wawancara.

Jenis Data

Data yang disajikan diperoleh dari sumber-sumber data yang meliputi sumber data primer dan sumber data sekunder:

- a. Data Primer
Bahan Hukum Primer, yakni data yang diperoleh melalui peraturan perundang-undangan yakni Undang-undang Nomor 17 Tahun 2023 tentang Kesehatan, Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis.
- b. Data sekunder
Berupa dokumen-dokumen tertulis, peraturan perundang-undangan dan literatur-literatur yang berkaitan dengan objek penelitian ini.

HASIL DAN PEMBAHASAN

Implikasi Hukum Pidana Cyber Terhadap Perlindungan Rekam Medis Elektornik Di Rumah Sakit

1. Peraturan-Peraturan Terkait Perlindungan Data Kesehatan

Perlindungan data kesehatan di Indonesia semakin diperkuat dengan hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. UU ini secara tegas mengatur kewajiban rumah sakit dan fasilitas kesehatan dalam menjaga kerahasiaan serta keamanan data pribadi pasien, termasuk data rekam medis elektronik (RME). Dalam hukum pidana cyber, ancaman terhadap RME yang

menyebabkan kebocoran data pribadi pasien dapat dikenakan sanksi pidana sebagaimana diatur dalam Pasal 65 UU Perlindungan Data Pribadi. Keberadaan UU ini memberikan landasan hukum dalam menghadapi ancaman kejahatan siber di bidang kesehatan.

Dalam implementasinya, UU Perlindungan Data Pribadi tidak hanya berfokus pada perlindungan data pribadi secara umum, tetapi juga mencakup ketentuan spesifik terkait data sensitif seperti data kesehatan. UU Perlindungan Data Pribadi memberikan perlindungan terhadap data kesehatan pasien yang diakses secara elektronik, serangan cyber terhadap RME bisa menimbulkan dampak besar, termasuk gugatan hukum dari pasien terhadap rumah sakit jika terjadi kebocoran data. Hal ini menjadikan perlindungan data kesehatan sebagai isu prioritas dalam kebijakan di rumah sakit (Ratnasari & Nurdin, 2023).

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik turut menjadi landasan hukum yang penting dalam perlindungan data rekam medis elektronik. Penyelenggaraan sistem elektronik termasuk rumah sakit, wajib menjamin keamanan sistem elektronik rumah sakit dari segala bentuk ancaman cyber. Pidana cyber yang merusak integritas data pasien bisa dikategorikan sebagai pelanggaran pidana cyber yang dikenakan sanksi berdasarkan UU Perlindungan Data Pribadi (Ahmad & Damanik, 2022).

Implikasi hukum pidana terhadap pelanggaran privasi data rekam medis juga diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah mengalami beberapa perubahan, termasuk dengan hadirnya Undang-Undang Nomor 19 Tahun 2016 dan perubahan kedua UU Nomor 1 Tahun 2024. Berdasarkan Pasal 30 UU ITE, setiap tindakan akses ilegal terhadap data elektronik, termasuk RME, dapat dikenakan pidana penjara dan denda. Kasus kejahatan cyber sering terjadi pada bidang kesehatan menjadi semakin umum, sehingga adanya regulasi sangat penting untuk menekan risiko kebocoran data pasien.

Perlindungan data kesehatan memerlukan dukungan kebijakan internal rumah sakit. Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis memperkuat standar keamanan dalam pengelolaan RME. Kebijakan internal rumah sakit harus sesuai dengan standar yang ditetapkan oleh peraturan RME, termasuk penggunaan teknologi enkripsi dan pengelolaan akses terhadap RME. Kegagalan dalam menerapkan langkah-langkah keamanan menyebabkan rumah sakit bertanggung jawab secara perdata, pidana dan administrative (Utama, 2022).

Dari hal tersebut, peraturan-peraturan yang digunakan Rumah Sakit Mitra Medika Premier Medan terkait perlindungan data Kesehatan menerapkan peraturan yang merujuk pada Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, yang mengatur kerahasiaan rekam medis, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan data pribadi, Peraturan Menteri Kesehatan RI Nomor 24 Tahun 2022 tentang Rekam Medis, sebagai dasar perlindungan data pasien dan Kebijakan internal rumah sakit yang memperkuat kepatuhan terhadap peraturan di atas, termasuk standar operasional prosedur (SOP) pengelolaan rekam medis elektronik (RME).

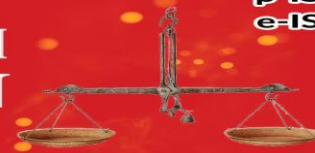
2. Implikasi Hukum Pidana Cyber Terhadap Perlindungan Rekam Medis Elektronik di Rumah Sakit

Rekam medis elektronik (RME) di rumah sakit merupakan inovasi penting dalam pengelolaan data kesehatan, namun juga membuka celah bagi kejahatan cyber. Tindakan cyber terhadap RME dapat mengakibatkan kebocoran data pasien yang bersifat privasi, yang berakibat adanya implikasi hukum pidana. Pelanggaran terhadap keamanan RME dapat dikenakan sanksi pidana Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang melindungi data pribadi, termasuk data kesehatan. Tindakan cyber seperti hacking dan ransomware terhadap RME juga dapat dikenakan sanksi dalam Undang-Undang Nomor 1 Tahun 2004 tentang Perubahan Kedua Undang-undang aNomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Implikasi hukum pidana cyber terhadap perlindungan RME diatur dalam Pasal 30 UU ITE yang menyatakan bahwa akses tanpa izin ke sistem elektronik, termasuk RME, merupakan tindak pidana yang dapat diancam dengan hukuman pidana. Kejahatan cyber di rumah sakit telah mengalami peningkatan secara signifikan, terutama dalam hal pencurian data pasien melalui metode *phishing* dan *malware*. Pelaku dapat dikenakan sanksi pidana berupa sanksi pidana penjara dan pidana denda sementara rumah sakit yang tidak memiliki sistem keamanan yang memadai juga dapat terkena sanksi administratif.

UU Perlindungan Data Pribadi memberikan perlindungan tambahan terhadap data kesehatan melalui mekanisme pengawasan yang lebih ketat. Rumah sakit wajib mengimplementasikan standar keamanan tinggi untuk melindungi RME dari akses yang tidak sah. Apabila rumah sakit gagal melaksanakan kewajibannya, rumah sakit dapat digugat secara perdata oleh pasien yang dirugikan, selain denda administratif. Hal ini menunjukkan pentingnya kebijakan internal rumah sakit dalam mencegah kebocoran data yang diakibatkan oleh kejahatan cyber (Saputra & Hamzah, 2022).

Selain sanksi pidana terhadap pelaku kejahatan cyber, implikasi hukum pidana juga dapat dialami oleh rumah sakit yang lalai dalam melindungi RME. Kegagalan rumah sakit dalam menerapkan



langkah-langkah keamanan yang memadai, seperti enkripsi dan pembatasan akses, dapat menyebabkan tuntutan hukum. Jika data pasien bocor akibat tindakan cyber yang bisa dicegah, rumah sakit dapat dituntut berdasarkan Pasal 26 UU Perlindungan Data Pribadi dan Pasal 32 UU ITE, yang mengatur tanggung jawab penyelenggara sistem elektronik (Kartika, 2023).

Perkembangan teknologi dan tindakan cyber diperlukan adanya peningkatan regulasi hukum pidana cyber dalam melindungi RME. Regulasi yang ada sangat diperlukan untuk mengantisipasi ancaman terbaru terhadap data kesehatan. Penegakan hukum yang lebih tegas dan pengawasan yang lebih ketat, diperlukan untuk memastikan bahwa RME terlindungi dari kejahatan cyber yang semakin canggih.

Dari hasil wawancara, bentuk pelanggaran keamanan data kesehatan yang mungkin terjadi adalah:

- a. Akses Tidak Sah (*Unauthorized Access*): Ketika login petugas kesehatan yang tidak hadir dititipkan pada petugas kesehatan lainnya untuk menggantikan pengentryan data.
- b. Pengambilan Data: Data pasien digunakan oleh pihak tidak berwenang misalnya foto hasil laboratorium.

Kendala Dan Hambatan Dalam Melindungi Rekam Medis Elektronik Di Rumah Sakit Mitra Medika Premier Medan

1. Keuntungan Dan Tantangan Penggunaan Rekam Medis Elektronik di Rumah Sakit Mitra Medika Premier Medan

Penggunaan rekam medis elektronik (RME) di rumah sakit menawarkan banyak keuntungan dan tantangan, salah satunya adalah efisiensi dalam pengelolaan data pasien. RME memudahkan akses informasi kesehatan pasien bagi dokter sebagai tenaga medis dan tenaga kesehatan lainnya, sehingga mempercepat pengambilan keputusan. Selain itu, RME juga dapat mengurangi kesalahan medis yang disebabkan oleh kelalaian pencatatan manual, sehingga meningkatkan kualitas pelayanan kesehatan di rumah sakit.

RME juga memberikan keuntungan dalam hal keamanan dan perlindungan data pasien. RME memungkinkan penerapan enkripsi dan akses terbatas yang hanya diberikan kepada pihak berwenang, sehingga dapat mengurangi risiko kebocoran data. Dengan adanya sistem audit trail, setiap akses dan perubahan data dapat dipantau, sehingga menciptakan transparansi dan akuntabilitas yang lebih baik dalam pengelolaan rekam medis. Keuntungan lain dari RME adalah peningkatan koordinasi antar tenaga medis. Dalam jangka panjang, penggunaan RME dapat meningkatkan efektivitas pelayanan kesehatan dan mengurangi waktu tunggu pasien, yang dapat meningkatkan kepuasan pasien terhadap layanan rumah sakit.

Perlindungan dan keamanan data Kesehatan dalam pengelolaan rekam medis elektronik di Rumah Sakit Mitra Medika Premier Medan dalam mengelola keamanan data dengan langkah-langkah berikut:

- a. Sistem Enkripsi: Semua data dalam rekam medis elektronik dienkripsi untuk mencegah akses tidak sah.
- b. Autentikasi: Hanya petugas yang berwenang yang dapat mengakses data melalui proses login dan password.
- c. Backup Berkala: Data rekam medis disimpan dalam sistem cadangan untuk mencegah kehilangan data akibat kerusakan sistem.
- d. Akses Terbatas: Pengelolaan hak akses hanya bagi petugas yang berwenang.

Dari perlindungan dan keamanan data kesehatan dalam pengelolaan rekam medis elektronik di Rumah Sakit Mitra Medika Premier Medan dalam mengelola keamanan data, terdapat berbagai keuntungan dan kelemahan dalam penggunaan Rekam Medis Elektronik di Rumah Sakit Mitra Medika Premier Medan. Adapun keuntungan dalam penggunaan Rekam Medis Elektronik di Rumah Sakit Mitra Medika Premier Medan yaitu:

- a. Efisiensi Proses: Mempermudah akses dan pencatatan data pasien.
- b. Akurasi Data: Mengurangi kesalahan manual dalam pencatatan.
- c. Keamanan yang Lebih Baik: Sistem elektronik memungkinkan pelacakan akses data.
- d. Kemudahan Kolaborasi: Data dapat diakses lintas SDM/departemen/unit kerja

Sedangkan kelemahan dalam penggunaan Rekam Medis Elektronik di Rumah Sakit Mitra Medika Premier Medan yaitu:

- a. Ketergantungan pada Teknologi: Gangguan teknis dapat menghentikan operasional.
- b. Ancaman cyber: Rekam medis elektronik menjadi target serangan.
- c. Biaya Implementasi Tinggi: Pemeliharaan sistem dan pelatihan membutuhkan investasi signifikan.

Tantangan besar dalam implementasi RME salah satunya adalah biaya yang tinggi untuk pemasangan dan pemeliharaan sistem. Rumah sakit sering kali menghadapi kendala anggaran yang signifikan ketika mencoba sistem RME, terutama rumah sakit yang lebih kecil atau di daerah terpencil. Biaya tersebut mencakup investasi awal, pelatihan tenaga medis, serta pemeliharaan rutin. Selain itu tantangan lain yang dihadapi adalah resistensi dari tenaga medis yang sudah terbiasa dengan sistem manual.

Tenaga medis dan tenaga kesehatan merasa kurang nyaman beralih ke RME karena perubahan memerlukan waktu untuk beradaptasi. Selain itu, beberapa tenaga medis dan tenaga kesehatan merasa bahwa penggunaan RME bisa mengganggu interaksi langsung dengan pasien karena waktu yang digunakan untuk mengoperasikan sistem.

Keamanan cyber juga menjadi tantangan utama dalam penggunaan RME. Kejahatan cyber seperti *hacking* atau *malware* dapat membahayakan kerahasiaan data pasien. Meski RME memberikan keamanan yang lebih baik dibandingkan sistem manual, tetap ada risiko kebocoran data jika tidak diimbangi dengan sistem keamanan yang kuat dan update berkala. Untuk itu, rumah sakit harus terus mengembangkan infrastruktur IT yang andal dan memadai guna melindungi data pasien.

3. Kendala Dan Hambatan Dalam Melindungi Rekam Medis Elektronik di Rumah Sakit Mitra Medika Premier Medan

Kendala dan hambatan dalam melindungi rekam medis elektronik (RME) di rumah sakit sangat beragam khususnya di Rumah Sakit Mitra Medika Premier Medan, salah satunya adalah kurangnya infrastruktur teknologi yang memadai. Banyak rumah sakit terutama di daerah terpencil atau yang memiliki anggaran terbatas, belum mampu menyediakan sistem keamanan yang kuat untuk melindungi data pasien secara optimal. Keterbatasan infrastruktur ini membuat sistem RME lebih rentan terhadap ancaman cyber dan kehilangan data akibat kegagalan teknis.

Hambatan lain adalah minimnya pemahaman dan kesadaran tentang pentingnya perlindungan data kesehatan di kalangan tenaga medis, tenaga kesehatan dan manajemen rumah sakit. Meskipun regulasi tentang perlindungan data sudah ada, seperti yang diatur dalam Undang-Undang Perlindungan Data Pribadi, pelaksanaannya masih lemah di beberapa rumah sakit. Banyak tenaga medis dan tenaga kesehatan yang belum memahami sepenuhnya pentingnya menjaga kerahasiaan rekam medis, yang berdampak pada potensi kebocoran data akibat kelalaian.

Masalah lain adalah tantangan finansial dalam menjaga keamanan RME. Pengadaan perangkat lunak keamanan yang canggih memerlukan biaya besar. Selain itu, biaya pemeliharaan dan pembaruan sistem keamanan secara berkala seringkali diabaikan oleh rumah sakit yang mengalami keterbatasan anggaran. Akibatnya, meskipun ada niat untuk menjaga kerahasiaan data, rumah sakit kerap kesulitan dalam menyediakan sumber daya yang cukup untuk keamanan siber (Anggraini & Putri, 2023).

Selain terkendala biaya, resistensi terhadap teknologi baru juga menjadi hambatan dalam melindungi RME. Tenaga medis dan tenaga kesehatan merasa tidak nyaman dengan penggunaan sistem elektronik dan lebih memilih metode manual. Hal ini menciptakan situasi di mana sebagian tenaga medis dan tenaga kesehatan menggunakan RME, sementara yang lain tetap bergantung pada sistem tradisional, sehingga menyebabkan tidak konsisten dalam perlindungan data dan meningkatkan risiko kebocoran.

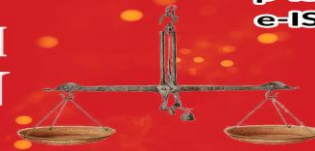
Di sisi lain, kurangnya kebijakan dan regulasi yang terintegrasi secara baik juga menjadi penghambat dalam perlindungan RME. Meskipun terdapat berbagai undang-undang terkait perlindungan data kesehatan, implementasi di lapangan sering kali kurang efektif. Tidak adanya panduan yang jelas mengenai pengelolaan keamanan data di tingkat rumah sakit menyebabkan berbagai kebijakan yang diterapkan tidak konsisten, membuat data pasien lebih rentan terhadap penyalahgunaan.

Ancaman cyber yang semakin canggih juga menjadi kendala besar. Dengan perkembangan teknologi, pelaku kejahatan cyber terus mengembangkan metode baru untuk mengakses data RME, seperti penggunaan *malware* yang sulit dideteksi. Keamanan cyber di banyak rumah sakit khususnya di Rumah Sakit Mitra Medika Premier Medan masih belum sepenuhnya siap menghadapi ancaman cyber, sehingga perlindungan RME membutuhkan biaya besar dalam keamanan dan pelatihan tenaga medis.

Upaya Pencegahan Pidana Cyber Dalam Melindungi Rekam Medis Elektronik Di Rumah Sakit Mitra Medika Premier Medan

1. Ancaman Keamanan Yang Dihadapi Dalam Pengelolaan Rekam Medis Elektronik di Rumah Sakit Mitra Medika Premier Medan

Ancaman keamanan dalam pengelolaan rekam medis elektronik (RME) di rumah sakit, termasuk di Mitra Medika Premier Medan, merupakan masalah yang sangat penting. Ancaman cyber menjadi salah satu ancaman utama yang akan dihadapi oleh rumah sakit. Ancaman seperti *malware*, *ransomware*, dan



phishing semakin sering terjadi pada sistem informasi kesehatan. Ancaman tersebut tidak hanya mengganggu operasi rumah sakit, tetapi juga bisa menyebabkan hilangnya data pasien.

Selain ancaman cyber, ancaman keamanan internal seperti kelalaian staf juga menjadi salah satu yang memengaruhi pengelolaan RME. Tenaga medis, tenaga kesehatan atau staf administrasi rumah sakit sering kali tidak sengaja membuka celah keamanan, misalnya melalui penggunaan password yang lemah atau pengaksesan data melalui perangkat yang tidak aman. Kelalaian seperti ini dapat menyebabkan kebocoran data yang seharusnya dilindungi dengan ketat.

Penggunaan perangkat mobile untuk mengakses rekam medis juga menimbulkan risiko tersendiri. Banyak tenaga medis dan tenaga kesehatan menggunakan perangkat pribadi seperti smartphone untuk mengakses data pasien, yang terkadang tidak memiliki sistem keamanan yang memadai. Hal ini memperbesar peluang terjadinya akses tidak sah atau pencurian data melalui perangkat mobile.

Rumah Sakit Mitra Medika Premier Medan juga menghadapi tantangan terkait pemenuhan standar keamanan data yang terus berkembang. Rumah sakit Mitra Medika Premier Medan masih berada dalam proses adaptasi terhadap regulasi keamanan data yang lebih ketat, seperti UU Perlindungan Data Pribadi. Implementasi teknologi yang memadai untuk mematuhi regulasi ini membutuhkan waktu dan biaya yang cukup besar.

Selain itu, integrasi antara sistem RME dengan sistem lain di rumah sakit juga bisa menjadi celah keamanan. Ketika berbagai sistem yang berbeda diintegrasikan untuk memfasilitasi sistem kerja rumah sakit, sering kali terjadi masalah yang mengakibatkan celah keamanan. Hal ini dapat dimanfaatkan oleh pelaku kejahatan cyber untuk menyerang sistem dan mengakses data pasien secara ilegal.

Untuk menghadapi ancaman-ancaman ini, Rumah Sakit Mitra Medika Premier Medan perlu terus memperbarui infrastruktur keamanan IT dan meningkatkan kesadaran staf terkait praktik keamanan. Salah satu cara untuk mengurangi ancaman tersebut adalah dengan memberikan pelatihan rutin kepada staf rumah sakit mengenai pentingnya keamanan data dan bagaimana cara menjaga kerahasiaan rekam medis pasien. Peningkatan kesadaran ini diharapkan dapat mengurangi risiko kebocoran data akibat kelalaian.

Beberapa bentuk pelanggaran yang mungkin terjadi dalam pengelolaan rekam medis elektronik di Rumah Sakit Mitra Medika Premier Medan adalah:

- a. Akses Tidak Sah (Unauthorized Access): Ketika login petugas kesehatan yang tidak hadir dititipkan pada petugas kesehatan lainnya untuk menggantikan pengentryan data.
- b. Pengambilan Data: Data pasien digunakan oleh pihak tidak berwenang misal foto hasil laboratorium.

Terdapat ancaman pencurian identitas dalam pengelolaan rekam medis elektronik di Rumah Sakit Mitra Medika Premier Medan akan Risiko pencurian data. Mungkin lebih tepatnya risiko karena rekam medis elektronik belum menggunakan double verifikasi misal dengan wajah atau scan finger sehingga dengan entry login atau password yang didapat maka setiap orang dapat mengaksesnya. Ancaman keamanan dalam pengelolaan rekam medis elektronik dalam pengelolaan rekam medis elektronik di Rumah Sakit Mitra Medika Premier Medan meliputi:

- a. Pengambilan data/Pencurian data
- b. Virus *Malware*; Menyebabkan kerusakan atau penyanderaan data.
- c. Kelalaian Pengguna: Kesalahan staf dalam penggunaan sistem.
- d. Penyalahgunaan akses oleh staf.

2. Upaya Pencegahan Pidana Cyber Dalam Melindungi Rekam Medis Elektronik di Rumah Sakit Mitra Medika Premier Medan

Upaya pencegahan pidana cyber dalam melindungi rekam medis elektronik (RME) di rumah sakit menjadi prioritas penting, mengingat meningkatnya ancaman cyber yang menargetkan data kesehatan. Salah satu langkah utama yang diambil oleh rumah sakit adalah memperkuat sistem keamanan digital melalui enkripsi data. Hal ini penting dalam melindungi data pasien dari akses tidak sah, di mana informasi yang dikirim melalui jaringan dienkripsi sehingga hanya pihak berwenang yang dapat membacanya. Hal ini mencegah pihak ketiga memanfaatkan data secara ilegal.

Upaya yang dilakukan Rumah Sakit Mitra Medika Premier Medan dalam melindungi data Kesehatan meliputi:

- a. Penguatan Infrastruktur Teknologi: Penerapan firewall, antivirus, dan enkripsi data.
- b. Audit Rutin: Memastikan sistem berjalan sesuai standar keamanan.
- c. Peningkatan Kesadaran Staf: Pelatihan reguler terkait perlindungan data.
- d. Update/pengembangan sistem teknologi informasi khususnya terkait security data.

Selain itu upaya peningkatan penggunaan rekam medis elektronik di Rumah Sakit Mitra Medika Premier Medan berfokus pada:

- a. Pelatihan Berkelanjutan: Membiasakan tenaga medis dengan sistem elektronik.
- b. Peningkatan Infrastruktur: Penyediaan perangkat keras dan jaringan yang memadai.
- c. Integrasi Data: Memastikan bridging data antar-sistem di rumah sakit.
- d. Feedback Pengguna/survei kepuasan user: Menggunakan masukan tenaga kesehatan untuk memperbaiki sistem.

Upaya Rumah Sakit Mitra Medika Premier Medan dalam peningkatan kesadaran dan pelatihan terhadap tenaga medis dan tenaga Kesehatan dalam pengelolaan rekam medis elektronik dilakukan melalui:

- a. Pelatihan Berkala: Program pelatihan rutin tentang manajemen rekam medis elektronik.
- b. Simulasi Keamanan Data: Menguji kesiapan staf terhadap ancaman siber.
- c. Sosialisasi Kebijakan: Penyebaran informasi tentang regulasi baru terkait data kesehatan.

Pelatihan rutin untuk tenaga medis, tenaga kesehatan dan staf rumah sakit Mitra Medika Premier Medan juga merupakan bagian penting dari upaya pencegahan. Pada umumnya terdapat berbagai tindakan kejahatan cyber di rumah sakit terjadi akibat kelalaian manusia, seperti penggunaan kata sandi yang lemah atau pengaksesan sistem melalui perangkat yang tidak aman. Oleh karena itu, pelatihan rutin mengenai kesadaran keamanan siber dapat membantu tenaga medis, tenaga kesehatan dan staf rumah sakit memahami pentingnya menjaga keamanan data dan mencegah serangan cyber.

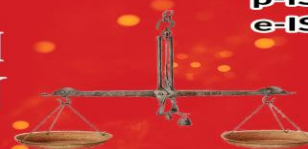
Upaya pencegahan lainnya yang juga penting adalah penerapan kebijakan akses terbatas. Akses ke rekam medis elektronik harus dibatasi hanya untuk personel yang berwenang. Setiap akses ke sistem harus dilacak dan diaudit secara berkala untuk memastikan bahwa tidak ada aktivitas yang mencurigakan. Dengan demikian, rumah sakit Mitra Medika Premier Medan dapat dengan cepat mendeteksi dan merespons potensi ancaman cyber yang berusaha mengakses data tanpa izin.

Sebagai upaya pencegahan pidana cyber dalam melindungi rekam medis elektronik di Rumah Sakit Mitra Medika Premier Medan, terdapat Kolaborasi antar lembaga penegak hukum dan sektor kesehatan dalam pengelolaan rekam medis elektronik di Rumah Sakit Mitra Medika Premier Medan yang dilakukan melalui Pelaporan jika ada pelanggaran data ke Komite Hukum Rumah Sakit dan ke Kementerian Kominfo dan Polri, Koordinasi Dinas Kesehatan dalam sosialisasi regulasi dan Keanggotaan PERSI dan ARSSI Sumut.

KESIMPULAN DAN SARAN

1. Peraturan-peraturan yang digunakan Rumah Sakit Mitra Medika Premier Medan terkait perlindungan data Kesehatan menerapkan peraturan yang merujuk pada Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, yang mengatur kerahasiaan rekam medis, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan data pribadi, Peraturan Menteri Kesehatan RI Nomor 24 Tahun 2022 tentang Rekam Medis, sebagai dasar perlindungan data pasien dan Kebijakan internal rumah sakit yang memperkuat kepatuhan terhadap peraturan di atas, termasuk standar operasional prosedur (SOP) pengelolaan rekam medis elektronik.
2. Dari perlindungan dan keamanan data kesehatan dalam pengelolaan rekam medis elektronik di Rumah Sakit Mitra Medika Premier Medan dalam mengelola keamanan data, terdapat berbagai keuntungan dan kelemahan dalam penggunaan Rekam Medis Elektronik di Rumah Sakit Mitra Medika Premier Medan.

Adapun keuntungan dalam penggunaan Rekam Medis Elektronik di Rumah Sakit Mitra Medika Premier Medan yaitu Efisiensi Proses: Mempermudah akses dan pencatatan data pasien, Akurasi Data: Mengurangi kesalahan manual dalam pencatatan, Keamanan yang Lebih Baik: Sistem elektronik memungkinkan pelacakan akses data dan Kemudahan Kolaborasi: Data dapat diakses lintas SDM/departemen/unit kerja. Sedangkan kelemahan dalam penggunaan Rekam Medis Elektronik di Rumah Sakit Mitra Medika Premier Medan yaitu: Ketergantungan pada Teknologi: Gangguan teknis dapat menghentikan operasional, Ancaman cyber: Rekam medis elektronik menjadi target serangan dan Biaya Implementasi Tinggi: Pemeliharaan sistem dan pelatihan membutuhkan investasi signifikan.



3. Beberapa bentuk pelanggaran yang mungkin terjadi dalam pengelolaan rekam medis elektronik di Rumah Sakit Mitra Medika Premier Medan adalah Akses Tidak Sah (Unauthorized Access): Ketika login petugas kesehatan yang tidak hadir ditiptikan pada petugas kesehatan lainnya untuk menggantikan pengentryan data dan Pengambilan Data: Data pasien digunakan oleh pihak tidak berwenang misal foto hasil laboratorium.
- Upaya yang dilakukan Rumah Sakit Mitra Medika Premier Medan dalam melindungi data Kesehatan meliputi: Penguatan Infrastruktur Teknologi: Penerapan firewall, antivirus, dan enkripsi data, Audit Rutin: Memastikan sistem berjalan sesuai standar keamanan, Peningkatan Kesadaran Staf: Pelatihan reguler terkait perlindungan data dan Update/pengembangan sistem teknologi informasi khususnya terkait security data.

DAFTAR PUSTAKA

- Anggraini dan Putri, 2023, *Hambatan Finansial dalam Menjaga Keamanan Rekam Medis Elektronik*, Jurnal Ekonomi Kesehatan.
- Gandomi A dan Haider, *Beyond the Hype: Big Data Concepts, Methods, and Analytics*, International Journal of Information, Management, 35 (2), 2015, 137-144.
- Kartika, 2023, *Regulasi Hukum Pidana Cyber Dalam Melindungi Rekam Medis Elektronik*, Jurnal Teknologi dan Hukum.
- M. Syamsudin, *Operasionalisasi Penelitian Hukum*, Jakarta, Raja Grafindo Persada, 2013, Hal. 25.
- Meher, Redyanto Sidi dan Irsyam Risdawati, *Penggunaan Data Kesehatan Pribadi Dalam Era Big Data: Tantangan Hukum dan Kebijakan di Indonesia*, Jurnal Ners Universitas Pahlawan, Volume 7 Nomor 2 Tahun 2023, hal. 864.
- Nurfadzilah H, *Penguatan Perlindungan Data Pribadi Dalam Layanan Kesehatan di Era Digital*, Jurnal Hukum dan Keadilan, 11 (1), 2021, 1-14.
- Raghupathi W dan Raghupathi V, *Big Data Analytics in Healthcare: Promise and Potential*, Helath Information Science and Systems, 2, 2014, 1-10.
- Rahayu Utama, 2022, *Implementasi Keamanan Rekam Medis Elektronik di Rumah Sakit*, Jurnal Manajemen Kesehatan.
- Ramli, Ahmad M, *Cyber Law dan Haki Dalam Sistem Hukum Indonesia*, Bandung: Refika Aditama, 2006, hlm 11.
- Ratnasari dan Nurdin, S, 2023, *Perlindungan Data Kesehatan dalam Era Digital*, Jurnal Hukum Kesehatan.
- Redyanto Sidi dan Ronnie Juliandri, *Urgensi Hukum Perikatan Terhadap Pasien yang Tidak Sadarkan Diri Dalam Pertolongan di IGD (Paper Topik Hukum Perdata Kesehatan)*, Jurnal Buletin Konstitusi, Volume 3, Nomor 1, Maret 2022, hal 18.
- Riski Darmawan, Redyanto Sidi dan Yasmirah Mandasari Saragih, *Perlindungan Hukum Terhadap Dokter Dalam Pelayanan Kesehatan Praktik Dokter Mandiri*, Jurnal Ners Universitas Pahlawan, Volume 7 Nomor 1 Tahun 2023, hal. 226.
- Saputra dan Hamzah, 2022, *Tinjauan Keamanan Data Elektronik dalam Perlindungan Rekam Medis*, Jurnal Hukum Kesehatan.
- Sulaiman, Robintan. *Cyber Crimes: Perspektif E- Commerce Crime*, Pusat Bisnis Fakultas Hukum: Universitas Pelita Harapan, 2002, hlm 13.

Surya Ahmad dan Damanik, T, 2022, *Ancaman Siber terhadap Data Pasien dan Perlindungannya*, Jurnal Teknologi Informasi.