

## KEAMANAN DAN KERAHASIAAN DATA MEDIS PASIEN DALAM IMPLEMENTASI REKAM MEDIS ELEKTRONIK : TINJAUAN SISTEMATIS

**Dini Puteri Astianto Pramesti<sup>1\*</sup>, Dumilah Ayuningtyas<sup>2</sup>, Riandi Verdi<sup>3</sup>**

Fakultas Kesehatan Masyarakat, Universitas Indonesia, Depok<sup>1,2,3</sup>

*\*Corresponding Author : diniputeriap@gmail.com*

### ABSTRAK

Keamanan dan Kerahasiaan data medis pasien merupakan salah satu aspek yang penting dalam sistem kesehatan di era digitalisasi, terutama dengan meningkatnya penggunaan rekam medis elektronik. Data medis pasien mencakup informasi penting yang digunakan dalam pengelolaan kesehatan individu yang terdiri dari 2 (dua) kategori utama yaitu data klinis dan data medis pasien. Rekam medis memiliki nilai rahasia yang harus dijaga fasilitas pelayanan kesehatan karena didalamnya terdapat riwayat pengobatan pasien dari awal sampai akhir pelayanan kesehatan. Tujuan penelitian ini adalah menganalisa keamanan dan kerahasiaan data medis pasien dalam implementasi rekam medis elektronik dan strategi yang dapat digunakan untuk meminimalisir terjadinya kebocoran data medis pasien menggunakan tinjauan literatur sistematis berskala luas. Tinjauan sistematis dilakukan dengan 4 (empat) database yaitu ProQuest, PubMed, ScienceDirect dan Scopus dengan kata kunci Electronic medical record, Electronic health record, EMR, security and confidentiality of medical data. Model PRISMA digunakan untuk menyaring judul dan abstrak, sehingga dari 412 total artikel yang ditemukan, didapatkan 8 artikel yang sesuai dengan kriteria inklusi. Kesimpulannya, Implementasi rekam medis elektronik harus dilakukan dengan mempertimbangkan berbagai aspek keamanan dan kerahasiaan supaya dapat memberikan manfaat yang maksimal.

**Kata kunci** : data medis, keamanan, kerahasiaan, rekam medis elektronik

### ABSTRACT

*Security and confidentiality of patient medical data is an important aspect of the health system in the era of digitalization, especially with the increasing use of electronic medical records. Patient medical data includes important information used in individual health management which consists of 2 (two) main categories, namely clinical data and patient medical data. Medical records have confidential value that must be maintained by health service facilities because they contain the patient's treatment history from the beginning to the end of health services. The aim of this research is to analyze the security and confidentiality of patient medical data in the implementation of electronic medical records and strategies that can be used to minimize leaks of patient medical data using a large-scale systematic literature reflection. A systematic review was carried out with 4 (four) databases, namely ProQuest, PubMed, ScienceDirect and Scopus with the keywords electronic medical record, electronic health record, EMR, security and confidentiality of medical data. The PRISMA model was used to filter titles and abstracts, so that of the 412 total articles found, 8 articles were obtained that met the inclusion criteria. In conclusion, the implementation of electronic medical records must be carried out by considering various aspects of security and confidentiality in order to provide maximum benefits.*

**Keywords** : medical data, security, confidentiality, electronic medical records

### PENDAHULUAN

Keamanan dan Kerahasiaan data medis pasien merupakan salah satu aspek yang penting dalam sistem kesehatan di era digitalisasi, terutama dengan meningkatnya penggunaan rekam medis elektronik. Data medis pasien mencakup informasi penting yang digunakan dalam pengelolaan kesehatan individu yang terdiri dari 2 (dua) kategori utama yaitu data klinis yang berkaitan langsung dengan riwayat medis dan kesehatan pasien, dan data administrasi yang

berkaitan dengan informasi pribadi pasien. Kedua kategori data medis pasien tersebut terekam dan tersimpan di dalam rekam medis elektronik. Rekam medis elektronik (RME) sendiri merupakan suatu perkembangan ilmu dan teknologi dimana penggunaan perangkat teknologi informasi untuk pengumpulan, penyimpanan, pengolahan dan pengaksesan data yang tersimpan pada rekam medis pasien di rumah sakit dalam suatu sistem manajemen basis data yang menghimpun berbagai sumber data medis (Handiwidjojo, 2015). Rekam medis memiliki nilai rahasia yang harus dijaga fasilitas pelayanan kesehatan karena didalamnya terdapat riwayat pengobatan pasien dari awal sampai akhir pelayanan kesehatan.

Tahun 2022 Kemenkes RI mewajibkan seluruh fasilitas pelayanan kesehatan (Fasyankes) yang ada di Indonesia untuk menyelenggarakan rekam medis elektronik dengan menerbitkan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 yang mana menggantikan PMK Nomor 269 Tahun 2008 tentang Rekam medis. Dalam PMK Nomor 24 tahun 2022 mempertimbangkan perkembangan teknologi digital pada saat ini yang mengakibatkan transformasi digitalisasi pelayanan kesehatan sehingga rekam medis perlu diselenggarakan secara elektronik dengan berprinsip keamanan dan kerahasiaan data dan informasi. Prinsip tersebut sejalan dengan isi PMK tentang rekam medis yang sebelumnya yaitu informasi tentang identitas, diagnosis, riwayat penyakit, riwayat pemeriksaan dan riwayat pengobatan pasien harus dijaga kerahasiaannya oleh dokter, dokter gigi, tenaga kesehatan tertentu, petugas pengelola dan pimpinan sarana pelayanan kesehatan.

Akan tetapi isi dalam PMK Nomor 24 Tahun 2022 pada pasal 28 menyebutkan bahwa fasilitas pelayanan kesehatan harus membuka akses seluruh isi rekam medis elektronik pasien ke Kementerian Kesehatan. Didukung dengan Pernyataan Ditjen Yankes Kemenkes, kedepannya fasyankes diwajibkan untuk terhubung dengan platform terintegrasi SATUSEHAT yang telah disediakan oleh Kementerian Kesehatan (Tarmizi, 2022). Platform SATUSEHAT merupakan ekosistem pertukaran data kesehatan (HIE: *Health Information Exchange*) yang menghubungkan sistem informasi atau aplikasi dari seluruh anggota ekosistem digital kesehatan Indonesia termasuk fasyankes, regulator, penjamin dan penyedia layanan digital (DTO Kemenkes, 2024). Secara sederhana platform SATUSEHAT ini bertujuan untuk mengintegrasikan data pelayanan kesehatan di seluruh Indonesia dengan pendekatan berbasis teknologi sehingga memungkinkan pasien, tenaga medis dan tenaga kesehatan untuk mengakses dan berbagi informasi medis dengan lebih efisien dan transparan.

Pada tahun 2023 Kementerian kesehatan RI resmi meluncurkan rekam medis elektronik yang terintegrasi dari hulu di SATUSEHAT Platform hingga hilir di SATUSEHAT Mobile (Tarmizi, 2023) yang mana nantinya masyarakat dapat mengakses resume medis pribadi miliknya secara mandiri dan online di SATUSEHAT Mobile. Hal tersebut memang memungkinkan dilakukan karena dalam PMK tentang rekam medis yang sebelumnya (PMK Nomor 269 Tahun 2008) disebutkan bahwa isi rekam medis dapat dibuka dalam hal permintaan institusi/lembaga berdasarkan ketentuan perundang-undangan dan sebelumnya atas persetujuan pasien sendiri. Permasalahan yang kemudian akan dihadapi adalah dengan kemudahan akses isi rekam medis elektronik tersebut memunculkan pertanyaan terkait keamanan dan kerahasiaan data medis pasien. *Health Insurance Portability and Accountability Act* (HIPAA) telah mengatur terkait keamanan dan kerahasiaan informasi khususnya dibidang kesehatan, terdapat beberapa hal yang harus dipenuhi sebagai berikut : 1) Memastikan kerahasiaan, integritas dan ketersediaan semua informasi kesehatan yang dilindungi dalam membuat, menerima, mempertahankan atau mentransmisikan informasi kesehatan; 2) melindungi terhadap ancaman atau bahaya yang diantisipasi secara wajar; 3) melindungi dari penggunaan atau pengungkapan informasi yang diantisipasi secara wajar berdasarkan peraturan privasi; 4) memastikan kepatuhan oleh tenaga kerjanya (Tiorentap & Hosizah, 2020). Sedangkan ISO/IEC 27001:2013 menyatakan bahwa acuan standar sistem manajemen keamanan informasi yang dikeluarkan oleh "International Organization for Standardization and

*International Commission*" terdiri dari *confidentiality* (kerahasiaan), *availability* (ketersediaan) dan *integrity* (integritas) (Ardianto *et al*, 2024).

Penerapan rekam medis elektronik memiliki banyak manfaat tetapi juga memiliki tantangannya tersendiri, salah satunya pada aspek keamanan dan kerahasiaan data. Gupta *et al* (2023) dalam Indriyajati *et al* (2023) menyatakan di era digital ini tidak ada yang aman, penyerang dapat mencuri data kesehatan dan data medis pasien berbasis *B2B* yang disimpan di *server cloud* untuk memodifikasi data untuk keuntungan pribadi. Samandari (2019) dalam Prisusanti *et al* (2022) menyatakan hal yang serupa bahwa transaksi elektronik masih menjadi hal yang berisiko di Indonesia karena dapat memunculkan permasalahan terkait keamanan dan kerahasiaan data, terutama jika terjadi kerusakan pada sistem atau biasa disebut *breakdown*. Meskipun secara keseluruhan, rekam medis elektronik dapat mempercepat kinerja tenaga medis dan tenaga kesehatan serta lebih bisa diandalkan dalam hal backup data, namun risiko terjadinya pembobolan data pada rekam medis elektronik memiliki peluang lebih tinggi dan cepat (Prisusanti *et al*, 2022 dalam Li, 2019). Ancaman terhadap keamanan dan kerahasiaan data medis pasien tersebut dapat memunculkan atau menimbulkan permasalahan etik dan hukum dalam implementasi rekam medis elektronik. Hal tersebut dapat merugikan fasilitas pelayanan kesehatan dan Kementerian Kesehatan serta membahayakan pasien sebagai pemilik informasi medis tersebut (Tedjasukmana & Riswadi, 2021).

Penelitian ini bertujuan untuk menganalisa keamanan dan kerahasiaan data medis pasien dalam implementasi rekam medis elektronik dan strategi yang dapat digunakan untuk meminimalisir terjadinya kebocoran data medis pasien menggunakan tinjauan literatur sistematis berskala luas.

## METODE

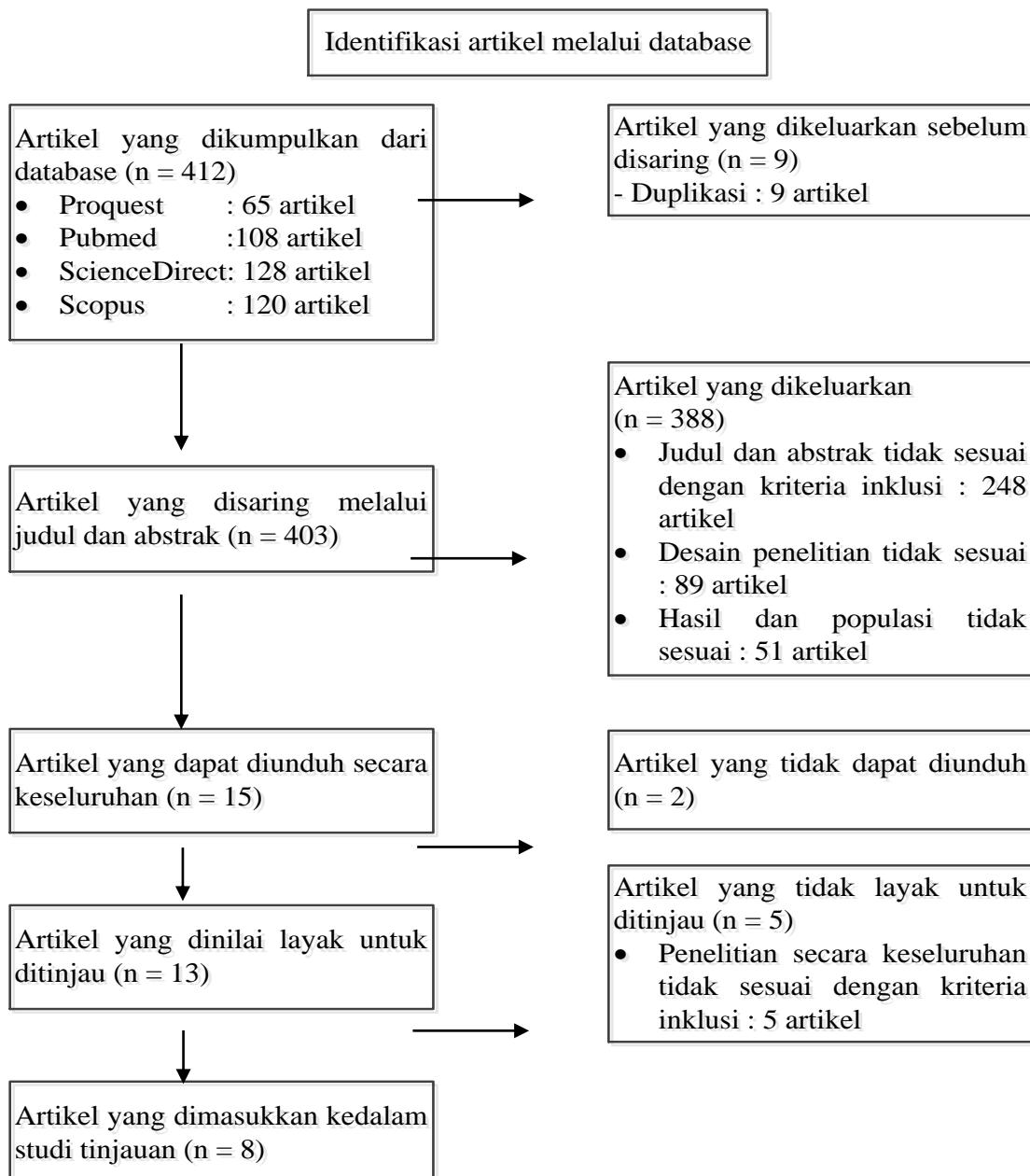
Menggunakan metode penelitian tinjauan literatur sistematis dengan mengikuti pedoman PRISMA (*Preferred Reporting Item for Systematic Reviews*) untuk mengeksplorasi dan mengidentifikasi keamanan dan kerahasiaan data medis pasien yang terdokumentasi dalam rekam medis elektronik. Database yang digunakan dalam penelitian ini adalah ProQuest, PubMed, ScienceDirect dan Scopus dengan kata kunci Electronic medical record, Electronic health record, EMR, security and confidentiality of medical data, Dimana peneliti akan meninjau literatur menggunakan pendekatan prioritas dan pengecualian yang dilakukan secara berurutan.

Adapun kriteria inklusi dalam penelitian ini adalah artikel dari berbagai negara yang menggunakan Bahasa Inggris dan Bahasa Indonesia dengan judul dan isi yang relevan dengan topik yang membahas tentang keamanan dan kerahasiaan data medis pasien yang terdokumentasi dalam rekam medis elektronik. Artikel yang digunakan sebagai literatur memiliki rentang waktu publikasi maksimal 3 tahun terakhir dan artikel yang dapat diakses secara penuh. Tinjauan dalam penelitian ini dilakukan oleh ketiga peneliti dengan pembagian tugas sebagai berikut : peneliti kesatu dan peneliti ketiga akan meninjau serta menyaring judul dan abstrak untuk menentukan artikel yang telah dikumpulkan sudah relevan dengan topik penelitian, sementara peneliti kedua akan membantu menyelesaikan perbedaan yang terjadi. Semua peneliti yang terlibat berperan dalam mempelajari artikel yang dimasukkan dalam studi tinjauan, mensintesis data dan merangkum Kesimpulan dalam bentuk narasi.

## HASIL

Berdasarkan pencarian artikel yang telah dilakukan sebelumnya dari 4 (empat) database dan mengikuti pedoman PRISMA (*Preferred Reporting Item for Systematic Reviews*) sesuai dengan Gambar 1, diperoleh 412 artikel dari pencarian awal. Dilanjutkan pada tahap

penyaringan pertama, dimana terdapat 403 artikel yang teridentifikasi tanpa duplikasi dari keseluruhan artikel yang diperoleh. Penyaringan kedua melalui identifikasi judul dan abstrak mendapatkan 15 artikel yang sesuai dengan kategori inklusi yang telah ditetapkan sebelumnya, dimana sebanyak 51 artikel dikeluarkan karena hasil dan tujuan penelitiannya tidak sesuai, 89 artikel memiliki desain penelitian yang tidak sesuai dengan kriteria inklusi dan 248 artikel dikeluarkan karena judul dan abstrak tidak sesuai dengan kriteria inklusi. Selanjutnya sebanyak 2 artikel tidak dapat diunduh dan didapatkan 13 artikel dalam bentuk *full-text*. Kemudian kami meninjau sebanyak 3 artikel yang tidak berfokus pada keamanan dan kerahasiaan data medis pasien. Pada tahap akhir diperoleh 10 artikel yang paling sesuai untuk dimasukkan dalam tinjauan literatur sistematis ini, seperti yang dijelaskan pada gambar 1.



Gambar 1. Diagram Alur Pemilihan Artikel Untuk Tinjauan Sistematis (PRISMA)

**Tabel 1. Tinjauan Artikel**

Judul	Penulis	Tahun Penelitian	Hasil Penelitian	Strategi dan Inovasi
BYOD security behaviour and preferences among hospital clinicians – A qualitative study	Wani, T., A. et al	2024	<p>Bring Your Own Device (BYOD) mengacu pada penggunaan perangkat pribadi seperti laptop, tablet atau smartphone oleh tenaga medis dan tenaga kesehatan dalam melakukan pelayanan kesehatan salah satunya pengisian rekam medis elektronik. Penggunaan BYOD menimbulkan banyak tantangan karena kontrol yang terbatas atas perangkat pengguna dan tindakan pengguna serta perilaku keamanan untuk melindungi data kesehatan milik rumah sakit.</p> <p>Hasil penelitian berfokus pada perilaku dan preferensi keamanan BYOD oleh tenaga medis dan tenaga kesehatan dengan 3 (tiga) topik inti yaitu teknologi, kebijakan dan SDM.</p> <p><b>Teknologi :</b>            Kontrol keamanan yang diterapkan oleh rumah sakit untuk melindungi personal health information (PHI) dengan cara Perangkat pribadi tenaga kesehatan telah didaftarkan ke rumah sakit sebelum diberikan izin untuk mengakses aplikasi atau layanan rumah sakit, dalam hal autentifikasi rumah sakit menerapkan autentifikasi dua faktor pada perangkat pribadi dengan OTP yang dikirimkan ke ponsel atau menggunakan microsoft autentikator, sistem masuk tunggal juga digunakan bersama dengan autentifikasi mutifaktor di beberapa rumah sakit untuk menyederhanakan akses ke layanan rumah sakit berdasarkan login satu kali.            Rumah sakit memiliki kontrol keamanan jaringan yang kuat seperti firewall yang memastikan bahwa perangkat pribadi di dalam atau di luar rumah sakit tidak membawa malware atau virus apapun ke dalam jaringan rumah sakit. Beberapa rumah sakit tidak mengizinkan tenaga medis dan tenaga kesehatan untuk mengakses layanan terkait pasien dari jarak jauh pada perangkat pribadi untuk menjaga kerahasiaan pasien.</p> <p><b>Kebijakan</b>            Rumah sakit memiliki kebijakan terkait Teknologi Informasi yang umum seperti kebijakan penggunaan yang dapat diterima atau kebijakan penggunaan internet yang menyoroti pentingnya menjaga informasi pasien dan sebagian besar kebijakan mengarah ke pedoman dasar dan umum sedangkan pedoman khusus untuk</p>	<p>Mencatat nomor IMEI setiap perangkat pribadi yang digunakan oleh tenaga medis dan tenaga kesehatan</p>

		<p>penggunaan perangkat pribadi, pengetahuan tentang praktik atau proses keamanan BYOD masih kurang.</p>	
		<p><b>Sumber Daya Manusia (SDM)</b> Pelatihan terkait keamanan BYOD sangat penting dan bermanfaat bagi tenaga medis dan tenaga kesehatan, seperti dapat meningkatkan keselamatan dan keamanan rumah sakit serta data pribadi secara produktif dan dapat memperkenalkan keamanan siber dalam pelatihan klinis untuk dokter generasi baru</p>	
<p><b>Effective privacy protection strategies for pregnancy and gestation information from electronic medical records: Retrospective Study in a national health care data network in china</b></p>	<p>Liu, C. <i>et al</i> 2024</p>	<p>Semua data pasien dalam penelitian diambil dari database CRDS yang mencakup catatan dari 19 rumah sakit berdasarkan kriteria inklusi yaitu pasien perempuan berusia 14 sampai dengan 50 tahun dan periode 1 januari 2010 sampai dengan 31 desember 2020, total 1.110.053 pasien dipilih sebagai sampel rekam medis elektronik. Selanjutnya peneliti secara acak memilih 1000 rekam medis elektronik pasien kehamilan untuk desensitisasi data statis guna membuat sampel rekam medis elektronik yang ditutupi. Aksesibilitas rekam medis elektronik mengarah pada kesadaran perlindungan privasi yang tidak merata diantara pengguna rekam medis elektronik yang berbeda sehingga pentingnya meode perlindungan privasi yang andal. Pada tahun 2021, undang-undang perlindungan informasi pribadi republik rakyat tiongkok mulai berlaku, yang mengklasifikasi hak dan tanggung jawab terkait penggunaan informasi pribadi. Akan tetapi, hanya sedikit atau tidak ada upaya untuk memenuhi standar tertinggi kebijakan tersebut. Dibandingkan dengan metode inklusi pasien berbasis diagnosis tradisional, metode Extraction Protocol of Pregnancy and Gestation Information (EPPGI) memberikan hasil yang lebih akurat secara praktis. Baik untuk catatan berbasis pasien maupun kunjungan, EPPGI mengekstraksi FRA secara signifikan lebih banyak dengan tingkat presisi yang tinggi. Dari perspektif manajemen aset data, mengukur risiko kebocoran privasi sangat penting berdasarkan undang-undang perlindungan informasi pribadi yang ketat.</p>	<p>Desensitisasi data rekam medis elektronik sangat penting untuk meminimalisir kebocoran data medis pasien. Penggunaan metode EPPGI lebih memberikan hasil yang akurat dan baik daam perlindungan data medis pasien kebidanan dan gestasi.</p>
<p><b>Factors influencing the sharing of personal health data based on the integrated theory of privacy calculus and</b></p>	<p>Shi, J. <i>et al</i> 2023</p>	<p>Sebanyak 2400 kuesioner didistribusikan dan 2060 kuesioner yang dikumpulkan valid (tingkat respon 85,83%). Sebagian besar responden tidak yakin apakah mereka pernah mengalami kebocoran informasi kesehatan pribadi 50,24% (1035/2060).</p>	<p>Pembuatan kebijakan dalam bentuk undang-undang perlindungan data pribadi</p>

theory of planned behaviors framework: results of a cross-sectional study of chinese patients in the yangtze river delta	Pasien yang mengalami kebocoran informasi kesehatan pribadi dan kunjungan rumah sakit tersier lebih cenderung berbagi informasi kesehatan mereka dengan penyedia layanan kesehatan. Karakteristik demografis lainnya seperti usia, jenis kelamin, tingkat pendidikan, pendapatan, status kesehatan yang dirasakan atau tempat tinggal tidak mempengaruhi kemauan untuk berbagi informasi kesehatan.  Penelitian ini menunjukkan bahwa risiko membagikan informasi kesehatan pribadi yang dirasakan lebih besar daripada manfaat yang dirasakan, pasien memiliki kekhawatiran yang kuat tentang berbagi data dan menyadari masalah perlindungan privasi. Lebih dari separuh sampel menyatakan sikap negatif terhadap pembagian informasi kesehatan pribadi, yang menunjukkan bahwa individu menjadi semakin sadar akan pentingnya menjaga informasi pribadi mereka.  Pasien khawatir tentang organisasi yang mengungkapkan, mentransfer dan menjual informasi pribadi mereka. Undang-undang pemerintah dianggap sebagai salah satu metode yang paling umum dan mendasar untuk melindungi data pribadi. Hipotesis bahwa persepsi efektivitas regulasi pemerintah memiliki dampak positif pada keinginan berbagi.	pasien dengan memperhatikan transparansi dan hak pasien.
Privacy concerns among the users of national patient portal: a cross-sectional population survey study	Kyytsonen, M. <i>et al</i> , 2024  Tujuan dari penelitian ini adalah untuk menjelaskan faktor-faktor apa saja yang berhubungan dengan kewaspadaan privasi di antara pengguna portal pasien. Di antara kelompok usia yang berbeda, kewaspadaan privasi lebih sering terjadi pada kelompok usia 50-59 tahun Pasien yang mengalami kesulitan keuangan lebih sering memiliki kewaspadaan privasi Pasien yang terbiasa menggunakan layanan telehealth dan merasa penggunaan layanan telehealth bermanfaat, jarang memiliki kewaspadaan privasi. Kepercayaan terhadap penyedia layanan kesehatan sebelumnya telah terbukti mengurangi ketakutan terhadap pembagian data privasi dan dukungan informasi untuk mendorong pembagian informasi kesehatan.	Pengadaan paduan tentang digital skill dan panduan penggunaan layanan telehealth Rekomendasi kebijakan, memerlukan tindakan untuk melindungi privasi pasien dan memberikan informasi yang transparan dan mudah dipahaim
Privacy-preserving search on medical data	Herres, B. <i>et al</i> , 2024  Penelitian ini membahas terkait algoritma pencarian privasi untuk data medis yang disimpan secara terpusat yang dirancang untuk memfasilitasi penelitian tetapi tetap menjaga kerahasiaan informasi medis pasien. Algoritma yang diusulkan memisahkan data medis dan data demografi pasien, menyimpannya dalam	Algoritma pencarian privasi data medis pasien dengan metode tiga pihak dua tahap.

The 21st century cures act and multiuser electronic health record access: potential pitfalls of information release	Anhalt, S.A. et al	2022	<p>komponen yang terpisah secara teknis dan organisasi. Pemisahan data dan algoritma pencarian terbukti efektif dalam menjaga privasi data medis pasien. Hasil penelitian menekankan pentingnya ukuran kohort minimum untuk mengurangi risiko penyerangan (<i>hacking</i>).</p>	<p>Penelitian ini membahas terkait <i>the 21st Century Cures Act</i> (Undang-undang penyembuhan abad 21) dan implikasinya terhadap akses rekam medis elektronik. <i>The 21st Century Cures Act</i> mewajibkan penyedia layanan kesehatan untuk memberikan akses yang bebas dan tidak terbatas kepada pasien terhadap informasi kesehatan milik mereka, yang bertujuan untuk meningkatkan transparansi dan kendali pasien dalam perawatan kesehatan. Akses yang lebih besar terhadap informasi kesehatan elektronik dapat membuat pasien merasa tidak nyaman dalam berbagi informasi sensitif jika wali atau orang tua memiliki akses juga terhadap informasi kesehatan elektronik mereka.</p> <p>Pengecualian privasi memungkinkan fasilitas layanan kesehatan untuk membatasi akses ke informasi kesehatan elektronik untuk melindungi privasi pasien, tetapi banyak fasnyakes yang tidak memahami sepenuhnya. Pengecualian privasi tersebut dapat menjadi hambatan dalam memberikan perawatan yang optimal karena harus memilah informasi sensitif dan menavigasi ketentuan pemblokiran informasi.</p>
Trust and health information exchanges: qualitative analysis of the intent to share personal health information	Busch-Casler, J et al	2023	<p>Tujuan dari penelitian ini adalah untuk mendapatkan pengetahuan yang dalam terkait masalah kepercayaan dalam rekam medis elektronik dan menjawab pertanyaan penelitian.</p> <p>Sebagian besar pasien, umumnya memiliki sikap positif terhadap pembagian catatan riwayat kesehatan pribadi mereka secara digital melalui rekam medis elektronik. Tingkat dasar kepercayaan pasien dalam pembagian catatan riwayat kesehatan pribadi mereka diciptakan melalui interaksi langsung dengan dokter yang merawat atau penyedia asuransi kesehatan.</p> <p>Faktor-faktor seperti pengalaman penggunaan teknologi, usia pasien, adanya kebijakan dan kecenderungan untuk percaya terhadap sistem yang ada berperan dalam pembentukan kepercayaan pasien terkait pembagian catatan riwayat kesehatan pribadi mereka.</p>	<p>Mengatur terkait penyedia layanan kesehatan mendapatkan hak untuk melakukan pengecualian atau pembatasan akses informasi kesehatan elektronik pasien Menetapkan sanksi bagi penyedia layanan kesehatan atau pengembang TI kesehatan yang melanggar ketentuan pemblokiran informasi, termasuk denda hingga \$1.000.000 per pelanggaran</p> <p>Melakukan edukasi ke pasien mengenai manfaat dan langkah-langkah keamanan informasi kesehatan Melakukan kalkulus privasi kepada pasien</p>

Understanding the perspectives of hajj city population on the confidentiality and privacy of digital health and medical information	Alhur, A	2024	<p>256 orang (49,42%) percaya bahwa mereka tidak memiliki hak untuk mengakses dan mengubah catatan medis mereka di Arab Saudi, sementara 169 orang (32,63%) yakin mereka memiliki hak ini, dan 93 orang (17,95%) menyatakan ketidakpastian.</p> <p>436 orang (55,40%) menyadari terkait undang-undang yang melarang penggunaan data medis tanpa persetujuan di Arab Saudi, sementara 168 orang (21,35%) tidak menyadari dan 170 orang (21,60%) tidak yakin.</p> <p>Orang dewasa yang lebih tua sering menunjukkan tingkat kepercayaan yang lebih rendah pada sistem kesehatan digital karena kekhawatiran tentang privasi dan pengalaman masa lalu dengan pelanggaran teknologi.</p> <p>Kemahiran komputer dan persepsi keamanan informasi kesehatan menunjukkan bahwa peningkatan keterampilan digital dapat meningkatkan kepercayaan individu terhadap keamanan informasi kesehatan.</p>	Meningkatkan literasi digital melalui program pendidikan yang ditargetkan
---	----------	------	--	---

## PEMBAHASAN

### Keamanan dan Kerahasiaan Data Medis Pasien Dalam Implementasi Rekam Medis Elektronik

Liu *et al* (2024) menyatakan bahwa aksesibilitas rekam medis elektronik mengarah pada kesadaran perlindungan privasi yang tidak merata diantara pengguna rekam medis elektronik yang berbeda sehingga pentingnya metode perlindungan privasi yang handal. Keamanan informasi dalam penggunaan informasi kesehatan elektronik dalam rekam medis elektronik sangat krusial. Pasien cenderung memiliki pandangan yang positif terkait membagikan catatan riwayat kesehatan pribadinya apabila keamanan informasi cukup memadai. Keamanan informasi meliputi perlindungan data dari ancaman dan pengelolaan kontrol serta adanya kebijakan keamanan yang efektif. Selain itu, agar pasien dapat percaya dengan informasi kesehatan elektronik, maka perlu dilakukan tindakan persuasif atau meyakinkan pasien bahwa mereka memiliki kontrol penuh atas catatan riwayat kesehatan pribadinya dan menjelaskan bahwa pasien memiliki hak untuk memberikan persetujuan atau tidak perihal pembagian catatan riwayat kesehatan pribadinya (Busch *et al*, 2023).

“First, do no harm” atau *nonmaleficence* merupakan prinsip dasar yang diajarkan kepada setiap penyedia layanan kesehatan. Prinsip ini menyarankan bahwa sebelum menerapkan intervensi medis apa pun, seseorang perlu mempertimbangkan potensi dampak negatif pada pasien. Menjaga privasi pasien di era digital juga merupakan kebutuhan etis dan hukum. Di Amerika Serikat, sudah terdapat undang-undang dengan nama *the 21st Century Cures Act* (Undang-Undang Penyembuhan Abad 21) yang bertujuan untuk meningkatkan akses pasien terhadap informasi kesehatan elektronik (EHI) dan mempromosikan interoperabilitas antar sistem EHR. Meskipun ada kemajuan dalam menyediakan akses yang lebih baik, terdapat kekhawatiran mengenai potensi risiko yang dihadapi pasien. Ketentuan ini mengharuskan penyedia layanan kesehatan untuk memberikan akses bebas kepada pasien atas EHI mereka. Namun, pengecualian untuk mencegah bahaya tidak berlaku untuk pasien di bawah umur karena aturan terkait pemblokiran informasi tidak berlaku dalam situasi dimana fasyankes ingin

membatasi akses orang tua atau wali dari pasien usia remaja terhadap informasi kesehatan elektronik mereka yang dapat memunculkan pelanggaran kerahasiaan dan mengurai kepercayaan pasien usia remaja (Anhalt, 2022).

Menurut Kyytsonen et al (2024), Kekhawatiran privasi dikaitkan dengan usia, kesulitan keuangan, keterampilan digital, kebutuhan akan panduan tentang telehealth dan penggunaan layanan telehealth. Orang berusia 50 hingga 59 tahun memiliki kekhawatiran privasi sedikit lebih sering dibandingkan dengan orang berusia 20 hingga 49 tahun. Mereka yang memiliki kesulitan keuangan, memiliki kekhawatiran privasi 1,6 kali lebih sering. Mereka yang memiliki keterampilan digital yang baik, tidak memerlukan panduan tentang telehealth, dan menemukan penggunaan layanan telehealth yang bermanfaat, memiliki kekhawatiran privasi lebih jarang. Hal tersebut selaras dengan hasil penelitian Alhur (2024) yang menyatakan Kemahiran dalam menggunakan computer berperan penting terkait persepsi keamanan informasi kesehatan. Orang yang memiliki kemahiran computer lebih tinggi merasa lebih aman mengenai perlindungan catatan riwayat pengobatan pribadi mereka. Selain hal tersebut, Wani (2024) menyatakan penggunaan BYOD atau Bring Your Own Device yang mengacu pada penggunaan perangkat pribadi milik tenaga medis dan tenaga kesehatan seperti laptop, tablet dan smartphone, menimbulkan banyak tantangan karena kontrol yang terbatas atas perangkat pengguna dan tindakan pengguna serta perilaku keamanan untuk melindungi data kesehatan milik rumah sakit.

### **Manfaat dan Tantangan Terkait Keamanan dan Kerahasiaan Data Dalam Rekam Medis Elektronik**

Fitur berbagi Informasi kesehatan dalam rekam medis elektronik memiliki potensi untuk meningkatkan kualitas pelayanan kesehatan dengan memberikan akses yang lebih baik dan cepat terhadap informasi kesehatan pasien sehingga memungkinkan keputusan klinis yang lebih tepat (Busch, 2023). Fitur berbagi informasi akan lebih berdampak apabila terdapat peraturan atau kebijakan yang dapat menjadi payung hukum. Seperti yang terlaksana di Amerika Serikat, terdapat undang-undang dengan nama *the 21st Century Cures Act* (Undang-Undang Penyembuhan Abad 21) memberikan pasien akses yang bebas dan tidak terbatas terhadap informasi kesehatan elektronik dan meningkatkan interoperabilitas antar sistem rekam medis elektronik sehingga memungkinkan informasi dapat diakses secara lebih efisien di berbagai platform (Anhalt, 2022). Meskipun pilihan pasien terkait privasi terbatas, tampaknya manfaat yang dirasakan lebih besar daripada risiko bagi pasien yang mempertimbangkan adopsi rekam medis elektronik (Kyytsonen, et al, 2024).

Selain rekam medis elektronik memiliki banyak manfaat dalam meningkatkan pelayanan kesehatan, tantangan terkait keamanan dan kerahasiaan data tetap akan ada. Salah satunya yaitu akses ke catatan riwayat kesehatan pribadi pasien yang bebas dan tidak terbatas dapat mengikis kepercayaan antara pasien dan fasyankes, terutama jika pasien merasa bahwa informasi sensitif mereka tidak aman dan dapat diakses oleh pihak yang tidak berwenang. Meskipun ada pengecualian privasi yang memungkinkan pasien meminta agar informasi mereka tidak dibagikan, tetapi masih banyak fasyankes yang tidak sepenuhnya memahami atau menerapkan pengecualian tersebut sehingga berpotensi melanggar kerahasiaan data medis (Anhalt, 2022).

### **Memperkuat Keamanan dan Kerahasiaan Data Pasien Dalam Rekam Medis Elektronik**

Adapun cara memperkuat keamanan dan kerahasiaan data pasien dalam rekam medis elektronik yakni : (1) Mencatat nomor IMEI setiap perangkat pribadi yang digunakan oleh tenaga medis dan tenaga kesehatan agar dapat melacak dalam penggunaan rekam medis elektronik (Wani, et al. 2024). (2) Menggunakan metode Extraction Protocol of Pregnancy and Gestation Information (EPPGI) untuk melakukan desensitisasi data rekam medis elektronik agar meminimalisir kebocoran data medis pasien (Liu, et al. 2024). (3) Menggunakan algoritma

pencarian privasi data medis pasien dengan metode tiga pihak dua tahap dalam sistem yang digunakan (Herres *et al*, 2024). (4) Melakukan edukasi ke pasien mengenai manfaat dan langkah-langkah keamanan informasi kesehatan serta melakukan kalkulus privasi kepada pasien (Busch, *et al* (2023) & Alhur (2024)). (5) Memberikan panduan tentang keterampilan digital dan penggunaan layanan telehealth bagi mereka yang menginginkannya, mungkin merupakan strategi yang relevan untuk mengurangi kewaspadaan privasi karena memiliki keterampilan yang diperlukan untuk penggunaan layanan telehealth sangat terkait. Oleh karena itu, rekomendasi kebijakan harus memerlukan tindakan untuk melindungi privasi pasien dan untuk memberikan informasi yang transparan dan mudah dipahami tentang tindakan tersebut bagi pengguna layanan (Kyytsonen, *et al* (2024) & Shi, *et al* (2023)). (6) Mengatur terkait penyedia layanan kesehatan mendapatkan hak untuk melakukan pengecualian atau pembatasan akses informasi kesehatan elektronik pasien supaya dapat mencegah bahaya pada pasien serta dapat melindungi kerahasiaan data pasien. Selain itu juga menetapkan sanksi bagi penyedia layanan kesehatan atau pengembang TI kesehatan yang melanggar ketentuan pemblokiran informasi, termasuk denda hingga \$1.000.000 per pelanggaran (Anhalt, 2022).

## KESIMPULAN

Meskipun rekam medis elektronik menawarkan manfaat dalam meningkatkan kualitas pelayanan kesehatan, tantangan terkait keamanan data medis pasien akan tetap ada. Usia, keterampilan digital dan kondisi keuangan pasien berpengaruh terhadap kepercayaan pasien terkait penggunaan rekam medis elektronik yang berprinsip interoperabilitas. Keamanan informasi medis dalam rekam medis elektronik sangat krusial untuk melindungi data medis pasien dari kebocoran data dan ancaman, sehingga harus diimbangi dengan perlindungan yang memadai untuk mencegah pelanggaran kerahasiaan data medis. Selain itu, terdapat beberapa langkah lainnya yang dapat diimplementasikan untuk melindungi keamanan dan kerahasiaan data medis pasien, seperti mencatat nomor IMEI perangkat pribadi yang digunakan oleh tenaga medis, mengatur hak akses penyedia layanan kesehatan untuk melindungi data pasien dari potensi bahaya dan melakukan edukasi kepada pasien mengenai keamanan informasi kesehatan. Implementasi rekam medis elektronik harus dilakukan dengan mempertimbangkan berbagai aspek keamanan dan kerahasiaan supaya dapat memberikan manfaat yang maksimal.

## UCAPAN TERIMAKASIH

Penulis mengucapkan terimakasih kepada semua pihak yang telah memberikan arahan, bimbingan, kritik dan saran dalam terselesaikannya artikel ini.

## DAFTAR PUSTAKA

- Alhur A. 2024. *Understanding the Perspectives of Hail City Population on the Confidentiality and Privacy of Digital Health and Medical Information*. Cureus, 16(7), e63752. <https://doi.org/10.7759/cureus.63752>
- Ardianto, E., T., Sabran. & Nurjanah, L. 2024. Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik Di Rumah Sakit X. Jurnal Rekam Medik dan Manajemen Informasi Kesehatan Vol 3 (2) pp 18 – 30. DOI: <https://doi.org/10.47134/rammik.v3i2.54>
- Arvisais-Anhalt, S., Lau, M., Lehmann, C. U., Holmgren, A. J., Medford, R. J., Ramirez, C. M., & Chen, C. N. (2022). *The 21st Century Cures Act and Multiuser Electronic Health Record Access: Potential Pitfalls of Information Release*. Journal of medical Internet research, 24(2), e34085. <https://doi.org/10.2196/34085>

- Busch-Casler, J., & Radic, M. (2023). Trust and Health Information Exchanges: Qualitative Analysis of the Intent to Share Personal Health Information. *Journal of medical Internet research*, 25, e41635. <https://doi.org/10.2196/41635>
- DTO Kemenkes RI. 2024. Apa Itu SATUSEHAT ?. Satusehat.kemkes.go.id [Diakses pada 14 Oktober 2024]. <https://satusehat.kemkes.go.id/platform/docs/id/playbook/introduction/>
- Handiwidjojo, W. 2015. Rekam Medis Elektronik. Jurnal Eksplorasi Karya Sistem Informasi dan Sains Vol 2 (1). pp 36 – 41
- Herres, B., Poschen, C., & Knorr, K. (2024). Privacy-Preserving Search on Medical Data. *Studies in health technology and informatics*, 316, 252–256. <https://doi.org/10.3233/SHTI240392>
- Indriyajati, F., Jawa, M.M.S.D. & Utomo, H. 2023. Analisis Keamanan Data Electronic Medical Record Digital Transformation Office (DTO) Kementerian Kesehatan Indonesia. *Sanskara Manajemen dan Bisnis* Vol 02(01) pp 59-66. DOI: 10.58812/smb.v2i01.
- Kemenkes RI. 2022. Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis. Jakarta: Kemenkes RI.
- Kyytönen, M., Vehko, T., Jylhä, V., & Kinnunen, U. M. (2024). Privacy concerns among the users of a national patient portal: A cross-sectional population survey study. *International journal of medical informatics*, 183, 105336. <https://doi.org/10.1016/j.ijmedinf.2023.105336>
- Liu, C., Jiao, Y., Su, L., Liu, W., Zhang, H., Nie, S., & Gong, M. (2024). Effective Privacy Protection Strategies for Pregnancy and Gestation Information From Electronic Medical Records: Retrospective Study in a National Health Care Data Network in China. *Journal of medical Internet research*, 26, e46455. <https://doi.org/10.2196/46455>
- Prisusanti, R. D & Afifah, L. 2022. Tinjauan Yuridis : Tantangan Kerahasiaan Rekam Medis Elektronik Berdasarkan Pada Permenkes Nomor 24 Tahun 2022. Prosiding Seminar Nasional Rekam Medis & Manajemen Informasi Kesehatan.
- Shi J, Yuan R, Yan X, Wang M, Qiu J, Ji X, Yu G. 2023. Factors Influencing the Sharing of Personal Health Data Based on the Integrated Theory of Privacy Calculus and Theory of Planned Behaviors Framework: Results of a Cross-Sectional Study of Chinese Patients in the Yangtze River Delta. *J Med Internet Res*, 25, e46562. DOI: 10.2196/46562
- Tarmizi, S., N. 2022. Fasyankes Wajib Terapkan Rekam Medis Elektronik. *Sehatnegeriku.kemkes.go.id* [Diakses pada 14 Oktober 2024]. <https://sehatnegeriku.kemkes.go.id/baca/umum/20220909/0841042/fasyankes-wajib-terapkan-rekam-medis-elektronik/>
- Tarmizi, S., N. 2023. Kemenkes Resmi Luncurkan Rekam Medis Elektronik Terintegrasi SATUSEHAT. *Sehatnegeriku.kemkes.go.id* [Diakses pada 14 Oktober 2024]. <https://sehatnegeriku.kemkes.go.id/baca/rilis-media/20231111/2044243/kemenkes-resmi-luncurkan-rekam-medis-elektronik-terintegrasi-satusehat/>
- Tedjasukmana, D. & Riswadi. 2021. Legal Aspects of Medical Records and Data Security for Patients in Hospitals. *ICLSSEE*. EAI. DOI: 10.4108/eai.6-3-2021.2306400.
- Tiorentap, D., R., A. & Hosizah. 2020. Aspek Keamanan Informasi dalam Penerapan Rekam Medis Elektronik di Klinik Medical Check-Up MP. 4th Proceeding Perspektif Implementasi FHIR. Pp 53 – 66. <https://prosiding.esaunggul.ac.id/index.php/FHIR/article/view/71/6>
- Wani, T. A., Mendoza, A., & Gray, K. (2024). BYOD security behaviour and preferences among hospital clinicians - A qualitative study. *International journal of medical informatics*, 192, 105606. <https://doi.org/10.1016/j.ijmedinf.2024.105606>