

Keamanan Sistem Rekam Medis Elektronik Untuk Menjamin Privasi Pasien Di Rumah Sakit Mitra Idaman Kota Banjar

Electronic Health Record System Security To Ensure Patient Privacy In Mitra Idaman Hospital Banjar City

Mochamad Fahmi^{1,*}, Sri Sugiarsi², Erna Adita Kusumawati³

^{1,2,3}Program Studi RMIK STIKes Mitra Husada Karanganyar
Jl. Brigjen Katamso Barat, Gapura Papahan Indah, Karanganyar, Jawa Tengah 57722

*e-mail korespondensi: mocfahmi026@gmail.com

Abstrak

Penelitian ini dilatarbelakangi oleh pentingnya menjaga keamanan dan privasi data pasien dalam sistem rekam medis elektronik (RME) di Rumah Sakit Mitra Idaman Kota Banjar. Dengan adopsi teknologi RME yang semakin luas, perlindungan terhadap informasi medis menjadi krusial untuk menghindari akses tidak sah dan manipulasi data. Tujuan penelitian ini adalah untuk mengeksplorasi implementasi keamanan sistem RME serta persepsi dan pengalaman pengguna dan pasien terkait keamanan dan privasi data medis mereka. Metode penelitian menggunakan pendekatan kualitatif dengan teknik wawancara mendalam kepada berbagai informan, termasuk pengelola layanan RME, pengguna sistem, dan pasien. Hasil penelitian menunjukkan bahwa RS Mitra Idaman Kota Banjar telah mengimplementasikan langkah-langkah keamanan yang solid melalui penggunaan kontrol akses ketat, teknologi jaringan yang aman, enkripsi data, serta audit dan backup data yang rutin. Pengguna dan pasien menyadari pentingnya penggunaan username dan password yang kuat serta transparansi dalam pengelolaan dan akses terhadap data medis mereka. Implikasi dari penelitian ini adalah peningkatan kesadaran dan kepercayaan pengguna dan pasien terhadap keamanan sistem RME di rumah sakit. Temuan ini juga memberikan landasan bagi penyedia layanan kesehatan untuk terus meningkatkan sistem keamanan dan privasi data, serta memberikan edukasi yang lebih baik kepada pengguna dan pasien tentang pentingnya menjaga kerahasiaan informasi medis.

Kata kunci: abstrak, kata kunci, petunjuk penulisan

Abstract

This research is motivated by the critical need to safeguard the security and privacy of patient data within Electronic Medical Records (EMR) systems at Mitra Idaman Hospital in Kota Banjar. With the increasing adoption of EMR technology, protecting medical information from unauthorized access and data manipulation is crucial. The objective of this study is to explore the implementation of EMR system security, as well as users' and patients' perceptions and experiences regarding the security and privacy of their medical data. The research employs a qualitative approach, conducting in-depth interviews with various stakeholders, including EMR service managers, system users, and patients. The findings reveal that Mitra Idaman Hospital has implemented robust security measures, including strict access controls, secure network technologies, data encryption, and regular data audits and backups. Users and patients are aware of the importance of using strong usernames and passwords, as well as the transparency in managing and accessing their medical data. The implications of this research include enhancing awareness and trust among users and patients regarding EMR system security at the hospital.

Keywords: abstract, keyword, writing guidelines

PENDAHULUAN

Rekam medis elektronik (RME) telah mengalami adopsi luas sebagai komponen penting dalam sistem pelayanan kesehatan global, menggeser perlahan rekam medis konvensional berbasis kertas. Sistem ini tidak hanya menyediakan akses yang lebih cepat dan efisien terhadap informasi pasien, tetapi juga memungkinkan integrasi data yang lebih baik antara penyedia layanan kesehatan, meningkatkan koordinasi perawatan, dan memfasilitasi pengambilan keputusan klinis yang lebih tepat waktu (Tsai dkk, 2020; Quinn dkk, 2019). Meskipun memberikan berbagai keuntungan ini, penerapan RME juga menghadirkan tantangan terkait dengan keamanan dan privasi data pasien.

Penelitian terdahulu telah menunjukkan bahwa sistem RME rentan terhadap berbagai risiko keamanan, termasuk akses tidak sah dan pelanggaran data yang dapat mengancam privasi pasien (Yeo & Banfield, 2022; Basil dkk, 2022). Insiden keamanan seperti pencurian identitas dan akses ilegal ke informasi medis sensitif telah menjadi perhatian utama dalam pengelolaan RME di berbagai setting pelayanan kesehatan (Janarthanan dkk, 2024). Selain itu, implementasi yang tidak tepat dan kurangnya kesadaran terhadap praktik-praktik keamanan yang baik juga dapat memperburuk masalah keamanan data pasien (Rahmatika, 2023).

Di samping tantangan umum ini, rumah sakit seperti RS Mitra Idaman Kota Banjar juga menghadapi masalah spesifik terkait dengan manajemen keamanan RME. Kurangnya pelaporan insiden keamanan secara konsisten dan kepatuhan yang rendah terhadap kebijakan keamanan data menjadi tantangan tersendiri dalam upaya untuk menjaga privasi pasien dengan efektif. Hal ini menunjukkan perlunya pendekatan yang lebih sistematis dan komprehensif dalam mengelola dan melindungi data medis elektronik di rumah sakit ini.

Fenomena ini menciptakan kesenjangan dalam penelitian, terutama dalam konteks rumah sakit swasta berskala menengah seperti RS Mitra Idaman di daerah pedesaan. Sebagian besar penelitian sebelumnya cenderung berfokus pada rumah sakit besar di kota-kota besar atau pada sistem kesehatan nasional yang lebih terstruktur (Belrado dkk, 2024; Rubiyanti, 2023). Oleh karena itu, masih ada kebutuhan yang besar untuk penelitian yang mendalam tentang keamanan dan manajemen risiko RME yang

sesuai dengan konteks rumah sakit swasta di daerah terpencil.

Gap dalam penelitian ini menyoroti urgensi untuk mengembangkan strategi yang dapat meningkatkan keamanan dan privasi data pasien di RS Mitra Idaman Kota Banjar. Penelitian ini dilakukan untuk mengatasi tantangan keamanan yang ada, tetapi juga untuk membangun kepercayaan masyarakat terhadap penggunaan RME dalam penyediaan layanan kesehatan. Dengan demikian, penelitian ini bertujuan untuk mengidentifikasi solusi yang efektif dan berkelanjutan guna memperkuat sistem keamanan RME di RS Mitra Idaman.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan fokus pada studi kasus di Rumah Sakit Mitra Idaman Kota Banjar, Jawa Barat. Pendekatan deskriptif kualitatif dipilih untuk menggambarkan secara mendalam faktor-faktor yang mempengaruhi keamanan sistem informasi, kebijakan penggunaan sistem informasi, dan kesadaran serta pemahaman terhadap sistem informasi rekam medis elektronik di lingkungan rumah sakit. Pengambilan data dilakukan melalui wawancara dengan berbagai pihak yang terlibat, disajikan pada **Tabel 1**, dengan tujuan untuk mendapatkan perspektif yang komprehensif dan representatif terhadap implementasi dan pengelolaan sistem RME di RS Mitra Idaman Kota Banjar.

Tabel 1. Informan Penelitian

Informan	Inisial Nama	Jabatan
1	AR	Pengelola IT
2	E	Legal Officer
3	I	Penanggungjawab Pendaftaran Pasien
4	B	Kepala Keperawatan
5	Y	Kepada Kebidanan
6	AY	Komite Komdis
7	S	Pasien
8	AN	Pasien
9	AT	Pasien
10	YR	Pasien

Penelitian ini berfokus pada analisis faktor-faktor kunci keamanan sistem informasi mengadopsi konsep dalam penelitian Subektiningsih dkk (2022) yang mencakup aspek *privacy*, *integrity*, *authentication*, *availability*, *access control*, dan *non-*

repudiation. Faktor kebijakan juga menjadi fokus, terutama dalam konteks regulasi dan kebijakan penggunaan RME di Indonesia, termasuk kewajiban rumah sakit untuk mematuhi Peraturan Menteri Kesehatan No. 24 Tahun 2022. Selain itu, faktor kesadaran dan pemahaman dari berbagai pihak yang terlibat dalam penggunaan RME juga menjadi bagian penting dari analisis. Penentuan sampel menggunakan pendekatan yang beragam untuk mencakup berbagai perspektif yang berbeda, yang kemudian dianalisis dengan menggunakan triangulasi sumber data untuk memastikan kebenaran informasi yang diperoleh. Hasil analisis akan disajikan melalui proses reduksi data, penyajian data, dan penarikan kesimpulan yang mendalam untuk memberikan gambaran yang akurat dan komprehensif terkait dengan implementasi dan manajemen keamanan RME di RS Mitra Idaman Kota Banjar.

HASIL

Deskripsi Objek Penelitian

Rumah Sakit Mitra Idaman Kota Banjar telah memulai implementasi sistem RME sejak tahun 2015, dimulai dengan pengembangan *software* internal yang disesuaikan dengan kebutuhan dan kemampuan dana yang tersedia. Sistem ini awalnya menggunakan *software* yang dikembangkan secara internal dan dioperasikan pada server komputer *Rainer* dengan sistem operasi *turnkey Tomcat*. Namun, dalam perkembangannya, pada bulan Agustus 2023, RS Mitra Idaman mengadopsi sistem RME dari pihak ketiga, yaitu *software teraMedic*. Keputusan untuk beralih ke *software teraMedic* didasarkan pada kemampuannya untuk memenuhi kebutuhan yang semakin kompleks dalam manajemen rekam medis elektronik, termasuk modul-modul seperti halaman awal, pendaftaran pasien, dan pencatatan medis pasien.

Selain dari segi *software*, RS Mitra Idaman juga menitikberatkan pada aspek keamanan dalam pengelolaan RME. Hal ini tercermin dalam implementasi kebijakan keamanan yang meliputi aspek fisik, jaringan, dan aplikasi. Secara fisik, kebijakan akses yang ketat diterapkan di ruang data center dan server untuk mencegah akses yang tidak sah. Di sisi jaringan, keamanan dipastikan melalui penggunaan protokol yang tepat seperti SSL

(*Secure Socket Layer*) dan TLS (*Transport Layer Security*) untuk transfer data, serta kontrol akses yang cermat untuk memastikan hanya pihak yang berwenang yang dapat mengakses informasi. Sedangkan dalam aplikasi, sistem *teraMedic* di RS Mitra Idaman harus memenuhi standar keamanan dengan memastikan setiap pengguna teridentifikasi dengan unik dan dapat mengakses data dengan aman melalui metode akses remote yang terjaga. Ini mencerminkan komitmen rumah sakit dalam menjaga kerahasiaan, keamanan, dan integritas data pasien sesuai dengan pedoman yang telah ditetapkan.

Perspektif Pengelola Layanan RME

Berdasarkan hasil wawancara dengan Informan 1 dan Informan 2, penelitian ini mengungkap beberapa aspek penting dalam pengelolaan RME. Informan 1 menjelaskan bahwa penggunaan *username* dan *password* adalah langkah pertama dan paling mendasar untuk menjaga privasi rekam medis elektronik. “*Nah, jadi begini, penggunaan username dan password itu penting banget dalam menjaga privasi dalam rekam medik elektronik. Jadi, setiap orang yang mau akses data medis harus punya username dan password masing-masing,*” ujar Informan 1. Hal ini menunjukkan bahwa kontrol akses yang ketat adalah fondasi utama untuk memastikan hanya individu yang berwenang yang dapat mengakses data medis pasien, sehingga privasi dan keamanan data tetap terjaga.

Lebih lanjut, Informan 1 menekankan pentingnya teknologi jaringan dan enkripsi data untuk meningkatkan privasi dan keamanan RME. “*Teknologi jaringan dan enkripsi data tuh jadi kunci penting buat meningkatkan privasi dalam pengelolaan rekam medik elektronik,*” kata Informan 1. Implementasi teknologi jaringan memastikan bahwa akses data medis hanya dilakukan melalui koneksi yang aman dan oleh individu yang berwenang. Selain itu, enkripsi data berfungsi untuk mengubah informasi medis menjadi kode yang tidak dapat dimengerti oleh pihak yang tidak berwenang, sehingga meskipun data tersebut dicegat atau diakses oleh pihak luar, isinya tetap tidak dapat dipahami tanpa kunci enkripsi yang tepat.

Dalam hal integritas data, Informan 1 dan Informan 2 menjelaskan bahwa sistem SIMRS memiliki mekanisme audit dan backup yang

ketat untuk menangani perubahan atau penghapusan data. *“Sistem biasanya punya cara khusus buat nangani perubahan atau penghapusan data oleh admin dalam rekam medis elektronik,”* ujar Informan 1. Sistem ini mencatat setiap tindakan yang dilakukan oleh administrator, memastikan bahwa setiap perubahan atau penghapusan data tercatat dengan baik. Selain itu, sistem juga melakukan backup data secara rutin, sehingga jika terjadi penghapusan atau perubahan data yang tidak diinginkan, data tersebut dapat dipulihkan dari cadangan. Informan 2 menambahkan, *“Nah, admin punya akses khusus buat ubah atau hapus data, tapi sistem pastiin cuma yang bener-bener punya izin yang bisa ngapa-ngapain.”*

Terakhir, Informan 1 dan Informan 2 menekankan pentingnya deteksi dan pencegahan manipulasi data oleh pihak yang tidak berwenang. *“Sistem punya trik khusus buat jaga data medis dari tangan-tangan yang nggak seharusnya,”* jelas Informan 2. Langkah-langkah yang diambil meliputi implementasi fitur jejak audit, kontrol akses yang ketat, enkripsi data, pemantauan aktivitas, dan validasi data secara rutin. Selain itu, integrasi dengan perusahaan lain seperti BPJS Kesehatan juga dijelaskan oleh kedua narasumber sebagai bagian dari upaya memastikan ketersediaan dan keamanan data. *“Integrasi sistem kayak gini bikin kerja sama antara rumah sakit, klinik, dan BPJS jadi lebih efisien dan bikin pelayanan kesehatan jadi lebih baik buat peserta BPJS,”* kata Informan 1. Implementasi langkah-langkah ini menunjukkan komitmen yang kuat dalam menjaga integritas dan keamanan data rekam medis elektronik, sehingga data medis pasien tetap aman dan terlindungi dari akses yang tidak berwenang.

Perspektif Pengguna RME

Keamanan sistem RME di RS Mitra Idaman Kota Banjar diidentifikasi berdasarkan hasil wawancara dengan Informan 3, Informan 4, Informan 5 dan Informan 6 sebagai pihak-pihak yang menggunakan sistem RME yang ada. Informan 3 menjelaskan bahwa penggunaan *username* dan *password* yang unik dan kuat merupakan langkah awal yang penting untuk mengamankan akses ke rekam medis elektronik. *“Oke, sebagai pengguna, paham banget soal pentingnya username dan password buat jaga privasi dalam rekam medik elektronik,”* ujarnya, menekankan pentingnya pemilihan *username*

dan *password* yang tidak mudah ditebak dan tidak dibagikan sembarangan. Selain itu, teknologi jaringan dan enkripsi data diterapkan untuk mengamankan transmisi dan penyimpanan data, sehingga hanya pihak yang berwenang yang dapat mengakses informasi sensitif tersebut. *“Teknologi jaringan dan enkripsi data ini bekerja sama buat jaga-jaga supaya data medismu tetap aman dari orang-orang yang nggak punya hak buat lihat,”* tambahnya.

Informan 3 juga menguraikan mekanisme yang ada untuk menangani perubahan atau penghapusan data oleh administrator serta langkah-langkah untuk mendeteksi dan mencegah manipulasi data oleh pihak yang tidak berwenang. Sistem dilengkapi dengan jejak audit yang sangat terperinci, mencatat setiap langkah yang dilakukan terhadap data medis, termasuk identitas pengguna, tindakan yang dilakukan, dan waktu tindakan tersebut terjadi. *“Dengan demikian, setiap perubahan atau akses yang mencurigakan bisa dengan cepat teridentifikasi dan ditindaklanjuti,”* jelasnya. Selain itu, pembatasan hak akses berdasarkan *user ID* dan *password* serta kebijakan pengaksesan data sesuai izin dari pemilik data atau pasien memastikan bahwa hanya pihak yang berwenang yang dapat mengakses informasi medis. *“Setiap orang punya akun khusus di sistem yang punya user ID dan password masing-masing... dengan sistem kayak gini, kita bisa jaga kerahasiaan data dan pastiin cuma yang berwenang aja yang bisa akses,”* katanya. Proses backup data secara teratur dan aman juga dilakukan untuk mengantisipasi peretasan data pasien dan memastikan ketersediaan informasi.

Informan 4 menjelaskan bahwa pemilihan *username* dan *password* yang kuat adalah langkah awal yang krusial. *“Ceritanya gini, sebagai pengguna, kita punya peran penting banget buat jaga privasi dalam rekam medik elektronik. Nah, salah satu caranya ya dengan pilih username dan password yang kuat dan nggak gampang ditebak,”* ujarnya. Hal ini disertai dengan larangan keras untuk membagikan informasi login kepada siapa pun kecuali kepada tenaga medis yang berwenang, memastikan bahwa akses terhadap data medis pasien hanya dilakukan oleh pihak yang tepat. Selain itu, teknologi jaringan dan enkripsi data digunakan untuk melindungi data dari akses tidak sah. *“Teknologi jaringan dan enkripsi data*

itu kayak alat keamanan super penting buat jaga data medismu tetap aman dan rahasia," jelasnya, mengilustrasikan bagaimana data diubah menjadi kode rahasia yang hanya bisa dibaca oleh pihak yang memiliki kunci dekripsi.

Lebih lanjut, Informan 4 menekankan pentingnya kontrol akses yang ketat dan jejak audit yang terperinci untuk menangani perubahan atau penghapusan data oleh administrator, serta mencegah manipulasi oleh pihak yang tidak berwenang. "Kontrol akses yang ketat juga menjadi pilar utama keamanan sistem ini," katanya, menambahkan bahwa hanya pengguna yang memiliki otorisasi sesuai dengan peran mereka yang dapat mengubah data medis. Sistem juga memonitor aktivitas secara *real-time* untuk mendeteksi aktivitas mencurigakan. "Kita punya fitur yang bisa rekam jejak aktivitas, jadi kita bisa lihat kalau ada yang mencurigakan," jelasnya. Proses *backup* data yang rutin dan aman, dengan enkripsi pada setiap salinan data, juga menjadi bagian integral dari strategi keamanan untuk mengantisipasi peretasan dan memastikan ketersediaan informasi. Selain itu, integrasi sistem informasi kesehatan dengan BPJS Kesehatan melalui protokol standar memungkinkan pertukaran data yang aman dan terkini, meningkatkan efisiensi layanan. "Jadi sistem informasi kesehatan biasanya terkoneksi dengan perusahaan lain, termasuk BPJS Kesehatan, melalui apa yang disebut sebagai integrasi sistem," ungkap Informan 4.

Informan 5 menegaskan pentingnya penggunaan username dan password yang kuat untuk menjaga privasi dalam rekam medik elektronik. "Gunakan kombinasi huruf, angka, dan karakter khusus yang nggak mudah ditebak. Hindari pakai yang sederhana atau informasi pribadi yang bisa diketahui orang lain," katanya dengan tegas. Hal ini merupakan langkah awal yang esensial dalam menjaga kerahasiaan data medis, sejalan dengan kebijakan untuk tidak membagikan informasi login kecuali kepada pihak berwenang seperti dokter atau petugas medis yang memerlukan akses.

Selain itu, teknologi jaringan dan enkripsi data dijelaskan sebagai benteng pertahanan utama untuk meningkatkan privasi dalam pengelolaan rekam medik elektronik. Informan 5 menjelaskan, "Teknologi jaringan itu kayak pagar yang melindungi data medismu dari akses yang nggak diizinkan. Sementara enkripsi data

itu kayak bikin kode rahasia dari data medismu biar cuma kamu dan dokter yang punya 'kunci' buat bukannya." Hal ini menunjukkan komitmen dalam memastikan bahwa data medis pasien tidak dapat diakses oleh pihak yang tidak berwenang, serta terlindungi dengan baik di dalam jaringan yang terhubung.

Dalam konteks integritas data, Informan 5 menjelaskan sistem yang komprehensif untuk menangani perubahan atau penghapusan data oleh administrator. "Sistem ini punya detektor kegiatan untuk mencatat setiap langkah perubahan atau penghapusan data oleh admin. Ada juga fitur kontrol akses yang ketat, memastikan hanya orang-orang dengan izin yang bisa mengakses dan mengelola data medis," ungkapnya. Proses pencatatan jejak (*audit trail*) dan *backup* data yang rutin menjadi bagian penting dalam strategi RS Mitra Idaman Kota Banjar untuk mendeteksi serta mengurangi risiko manipulasi data oleh pihak yang tidak berwenang.

Informan 6 menekankan pentingnya penggunaan username dan password yang aman sebagai langkah pertama dalam menjaga privasi. "Pilihlah username yang unik tapi mudah diingat, misalnya kombinasi antara nama dan angka yang kamu sukai. Jangan lupa juga untuk bikin password yang kuat, dengan campuran huruf besar-kecil, angka, dan simbol," ungkapnya. Dialog ini mencerminkan kesadaran akan pentingnya keamanan informasi dalam akses terhadap rekam medis elektronik.

Selanjutnya, Informan 6 menjelaskan bagaimana teknologi jaringan dan enkripsi data digunakan untuk meningkatkan privasi dalam pengelolaan rekam medis elektronik. "Teknologi jaringan itu kayak tembok pelindung di sekitar data medismu. Mereka ngecek siapa yang boleh masuk dan akses data, jadi cuma orang-orang yang punya izin aja yang bisa lewat," ujarnya. Pendekatan ini menggambarkan sistem perlindungan yang kokoh untuk mencegah akses yang tidak sah. Dia juga menyoroti peran enkripsi data dalam menjaga kerahasiaan informasi. "Enkripsi data itu kayak bikin data medismu jadi kode rahasia yang cuma bisa dimengerti sama dokter atau petugas medis yang punya 'kunci'. Jadi, walaupun ada orang iseng yang coba-coba ngintip, mereka nggak bakal bisa baca data medismu," paparnya.

Hasil wawancara dengan pengguna RME mengungkap keseriusan Rumah Sakit Mitra

Idaman Kota Banjar dalam mengamankan sistem rekam medis elektronik (RME) untuk melindungi privasi pasien. Langkah-langkah yang ditekankan antara lain pemilihan *username* dan *password* yang kuat untuk mengontrol akses, penerapan teknologi jaringan dan enkripsi data sebagai lapisan pertahanan utama, serta sistem audit yang detail untuk memantau setiap aktivitas yang dilakukan terhadap data medis. Pembatasan hak akses berbasis *user ID* dan *password*, bersama dengan kebijakan pengaksesan data sesuai izin dari pemilik data, juga menjadi fokus utama dalam menjaga kerahasiaan informasi sensitif. Proses backup data yang teratur dengan enkripsi menyempurnakan strategi keamanan untuk mengantisipasi risiko peretasan dan memastikan ketersediaan informasi yang kritis bagi pelayanan kesehatan.

Hal ini menunjukkan komitmen yang kuat dari Rumah Sakit Mitra Idaman Kota Banjar dalam menjaga integritas dan keamanan data pasien melalui implementasi teknologi dan kebijakan yang ketat, yang tidak hanya memenuhi standar keamanan data kesehatan nasional tetapi juga menawarkan perlindungan ekstra terhadap informasi medis yang sensitif.

Perspektif Pasien

Hasil wawancara dengan Informan 7 sebagai pasien menyoroti beberapa aspek penting terkait keamanan sistem RME di Rumah Sakit Mitra Idaman Kota Banjar. Informan 7 mengungkapkan bahwa dia memiliki sedikit pengetahuan tentang bagaimana data rekam medisnya disimpan dan diakses oleh penyedia layanan kesehatan, menunjukkan bahwa transparansi tentang prosedur ini mungkin perlu ditingkatkan untuk memberikan pemahaman yang lebih baik kepada pasien. Ketidakpastian ini juga tercermin dalam rasa percaya dirinya terhadap keamanan data, di mana Informan 7 mengungkapkan harapannya bahwa penyedia layanan telah mengimplementasikan langkah-langkah yang memadai untuk melindungi data rekam medisnya dari akses yang tidak sah. Namun, kebutuhan akan penjelasan yang lebih mendetail tentang keamanan data adalah penting untuk meningkatkan kepercayaan pasien terhadap sistem ini. Selain itu, Informan 7 menyuarakan ketidakpastiannya apakah telah diberi kesempatan untuk memberikan izin atau

menolak berbagi data rekam medisnya dengan pihak lain, menyoroti pentingnya kontrol pasien atas data pribadi mereka dan pemahaman yang lebih baik akan implikasi dari pilihan tersebut terhadap keamanan data.

Hasil wawancara dengan Informan 8 sebagai pasien mengungkapkan beberapa aspek yang penting terkait dengan keamanan sistem rekam medis elektronik (RME) di Rumah Sakit Mitra Idaman Kota Banjar. Informan 8 menyatakan bahwa tidak terlalu paham secara rinci bagaimana data rekam medisnya disimpan dan diakses oleh penyedia layanan tindakan, menunjukkan bahwa ada kebutuhan untuk meningkatkan pemahaman pasien tentang proses ini. Ketidakpastian ini juga tercermin dalam kepercayaannya terhadap langkah keamanan yang telah diimplementasikan oleh penyedia layanan, di mana Informan 8 mengungkapkan keraguannya terhadap keefektifan langkah-langkah tersebut mengingat adanya kasus pelanggaran data yang sering terjadi. Informan 8 juga menyoroti pentingnya transparansi dari penyedia layanan dalam menjelaskan secara jelas langkah-langkah konkret yang diambil untuk melindungi privasi data rekam medisnya. Namun demikian, Informan 8 menyatakan bahwa telah diberi kesempatan untuk memberikan izin terkait berbagi data rekam medisnya dengan pihak lain, dan dia memahami implikasi dari pilihan ini terhadap keamanan data. Informan 8 percaya bahwa dengan memberikan izin, informasi medisnya dapat digunakan secara efektif untuk manfaat perawatan kesehatannya, meskipun tetap waspada terhadap risiko keamanan yang terkait dengan berbagi informasi tersebut.

Hasil wawancara dengan Informan 9 sebagai pasien mengungkapkan bahwa dia memiliki pemahaman umum tentang bagaimana data rekam medisnya disimpan dan diakses oleh penyedia layanan tindakan. Informan 9 menyadari bahwa data tersebut disimpan dalam bentuk digital yang dilindungi dengan enkripsi dan memiliki akses terbatas kepada staf medis yang berwenang. Meskipun Informan 9 mengakui adanya langkah-langkah manajemen data yang aman, Informan 9 tetap merasa kurang yakin terhadap keefektifan tindakan keamanan yang diimplementasikan oleh penyedia layanan tindakan, terutama dalam menghadapi ancaman akses yang tidak sah. Kekhawatiran ini menunjukkan perlunya transparansi lebih lanjut

dari penyedia layanan dalam menjelaskan dengan detail langkah-langkah konkret yang mereka ambil untuk melindungi privasi dan keamanan data rekam medis pasien. Meskipun demikian, Informan 9 menyatakan bahwa telah diberi kesempatan untuk memberikan izin terkait berbagi data rekam medisnya dengan pihak lain, dan Informan 9 memahami implikasi dari pilihan ini terhadap keamanan data. Informan 9 percaya bahwa penyedia layanan tindakan telah mengambil langkah-langkah yang memadai untuk melindungi privasi dan kerahasiaan informasi medisnya, meskipun dengan perasaan waspada terhadap risiko yang terkait.

Hasil wawancara dengan Informan 10 sebagai pasien menunjukkan bahwa dia memiliki pemahaman yang cukup baik tentang bagaimana data rekam medisnya disimpan dan diakses oleh penyedia layanan kesehatan. Informan 10 percaya bahwa data tersebut disimpan secara elektronik dalam sistem manajemen rekam medis yang terencana dengan baik, dengan akses terbatas hanya kepada staf medis yang memiliki izin dan kebutuhan yang jelas. Informan 10 juga yakin bahwa penyedia layanan kesehatan telah mengimplementasikan tindakan keamanan yang memadai, termasuk protokol keamanan yang ketat, enkripsi data, dan sistem autentikasi ganda untuk melindungi privasi dan kerahasiaan informasi medisnya. Informan 10 telah diberikan kesempatan untuk memberikan izin terkait berbagi data rekam medisnya dengan pihak lain, dan memilih untuk memberikan izin karena keyakinannya bahwa hal ini akan meningkatkan perawatan kesehatannya. Meskipun menyadari risiko keamanan yang terkait dengan berbagi informasi medis, Informan 10 yakin bahwa langkah-langkah yang diambil oleh penyedia layanan kesehatan sudah cukup untuk melindungi data pribadinya.

Secara keseluruhan, analisis hasil wawancara ini menggambarkan tingkat kepercayaan dan pemahaman yang baik dari pasien terhadap keamanan sistem rekam medis elektronik di RS Mitra Idaman Kota Banjar

PEMBAHASAN

Penelitian ini mengungkap beberapa temuan kunci terkait dengan keamanan sistem RME di Rumah Sakit Mitra Idaman Kota

Banjar. Pertama, pentingnya penggunaan username dan password dalam menjaga privasi rekam medis elektronik sangat ditekankan. Penggunaan kombinasi yang kuat dari huruf besar-kecil, angka, dan simbol membantu mengamankan akses hanya untuk mereka yang berwenang, menjaga privasi pasien, dan mencegah akses tidak sah. Kedua, teknologi jaringan dan enkripsi data diidentifikasi sebagai kunci untuk meningkatkan privasi dalam pengelolaan rekam medis. Teknologi ini berfungsi sebagai lapisan pertahanan yang mengatur akses dan mengubah data medis menjadi kode-kode yang hanya dapat diakses oleh pihak yang berwenang, memastikan data tetap aman dan terlindungi.

Ketiga, sistem SRME di RS Mitra Idaman Kota Banjar memiliki mekanisme khusus untuk mengelola perubahan atau penghapusan data oleh administrator guna menjaga integritas data. Jejak audit dan kontrol akses ketat memainkan peran krusial dalam memastikan bahwa manipulasi data hanya dilakukan oleh pihak yang berwenang, dengan rutusnya backup data untuk mengantisipasi kehilangan informasi penting. Keempat, terhubungnya sistem informasi kesehatan dengan lembaga seperti BPJS Kesehatan melalui integrasi sistem menjadi penting untuk meningkatkan ketersediaan dan koordinasi data pasien, dengan keamanan data yang dijaga melalui langkah-langkah perlindungan yang ketat.

Dari hasil wawancara dengan pasien, terlihat bahwa tingkat pemahaman dan kepercayaan terhadap keamanan SRME bervariasi. Beberapa pasien merasa perlu untuk lebih memahami bagaimana data mereka disimpan dan diakses, sementara yang lain yakin bahwa langkah-langkah keamanan yang telah diimplementasikan oleh rumah sakit sudah memadai. Pasien juga mengakui hak pasien untuk memberikan izin atau menolak berbagi data rekam medis mereka dengan pihak lain, dengan kesadaran akan implikasi yang terkait dengan keamanan dan privasi data. Perbedaan ini menyoroti pentingnya edukasi yang terus menerus kepada pasien tentang perlindungan data dan hak mereka dalam pengelolaan rekam medis elektronik.

SIMPULAN

Penelitian ini mengungkap bahwa keamanan sistem RME di Rumah Sakit Mitra Idaman Kota Banjar telah diimplementasikan dengan serius melalui penggunaan teknologi jaringan yang aman, enkripsi data yang kuat, dan kebijakan kontrol akses yang ketat. Langkah-langkah ini bertujuan untuk memastikan bahwa hanya pihak yang berwenang yang dapat mengakses dan mengelola informasi medis pasien, menjaga privasi serta integritas data dengan baik. Temuan dari wawancara dengan pengelola layanan, pengguna, dan pasien menunjukkan variasi dalam pemahaman dan kepercayaan terhadap keamanan sistem, serta kebutuhan akan transparansi yang lebih besar terkait pengelolaan dan akses data medis.

Saran penelitian selanjutnya dapat melibatkan studi komparatif antara implementasi RME di rumah sakit yang berbeda untuk memahami faktor-faktor yang mempengaruhi keefektifan dan keamanan sistem yang dapat mencakup analisis mendalam terhadap kebijakan keamanan yang diterapkan, integrasi sistem dengan lembaga lain, serta persepsi dan pengalaman pengguna dalam mengakses dan memanfaatkan data medis elektronik.

REFERENSI

- Barbieri, C., Neri, L., Stuard, S., Mari, F., & Martín-Guerrero, J. D. (2023). From electronic health records to clinical management systems: How the digital transformation can support healthcare services. *Clinical Kidney Journal*, 16(11), 1878–1884. <https://doi.org/10.1093/ckj/sfad168>
- Basil, N. N., Ambe, S., Ekhaton, C., & Fonkem, E. (2022). Health records database and inherent security concerns: A review of the literature. *Cureus*, 14(10), e30168. <https://doi.org/10.7759/cureus.30168>
- Belrado, R. N., Harmendo, H., & Wahab, S. (2024). Analisis penggunaan rekam medis elektronik di rumah sakit. *Jurnal Penelitian Perawat Profesional*, 6(4). <https://doi.org/10.37287/jppp.v6i4.3039>
- Janarthanan, V., Kumaran, S., Nagrale, N. V., Singh, O. G., & Raj, K. V. (2024). Legal and ethical issues associated with challenges in the implementation of the electronic medical record system and its current laws in India. *Cureus*, 16(3), e56518. <https://doi.org/10.7759/cureus.56518>
- Kementerian Kesehatan. (2022). *Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis*. Jakarta: Kementerian Kesehatan.
- Lestari, S. (2021). *Peran rekam medis elektronik sebagai alat bukti transaksi terapeutik di rumah sakit* (Tesis magister, Program Studi Hukum, Universitas 17 Agustus 1945 Semarang).
- Quinn, M., Forman, J., Harrod, M., Winter, S., Fowler, K. E., Krein, S. L., Gupta, A., Saint, S., Singh, H., & Chopra, V. (2019). Electronic health records, communication, and data sharing: Challenges and opportunities for improving the diagnostic process. *Diagnosis (Berl)*, 6(3), 241-248. <https://doi.org/10.1515/dx-2018-0036>
- Rahmatika, C., Werman, W., Arrazy, M., & Abdillah, N. (2023). Security and confidentiality of medical record data in hospitals in the use of electronic medical records: Literature review. *Journal of Medical Record and Information Technology (JOMRIT)*, 1(1), 11. Retrieved from <https://jurnal.syedzasaintika.ac.id/index.php/jomrit>
- Ramadhanti, A. T. (2022). *Analisis aspek keamanan informasi pasien dalam penerapan rekam medis elektronik di Rumah Sakit PHC Surabaya* (Project Report). Politeknik Negeri Jember, Jember.
- Rubiyanti, N. S. (2023). Penerapan rekam medis elektronik di rumah sakit di Indonesia: Kajian yuridis. *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, 1(1), 179-187. <https://doi.org/10.59246/aladalah.v1i1.163>
- Salsabila, A. A. (2023). *Tinjauan aspek keamanan dan privasi rekam medis di pelayanan rawat jalan RSUD Dr.*

Soekardjo Kota Tasikmalaya (Diploma thesis). Politeknik Kesehatan Tasikmalaya.

Sofia, S., Ardianto, E. T., Muna, N., & Sabran, S. (2022). Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Fasilitas Kesehatan. *Jurnal Rekam Medik & Manajemen Informasi Kesehatan*, 1(2), 94-103.
<https://doi.org/10.47134/rmik.v1i2.29>

Subektiningsih, A., Eko Prasetyo, A. R., & Indrayani, R. (2022). Evaluasi aspek keamanan informasi sistem penilaian mahasiswa magang menggunakan metode Failure Mode and Effect Analysis. *Jurnal Teknik Komputer AMIK BSI*, 8(2).
<https://doi.org/10.31294/jtk.v4i2>

Tsai, C. H., Eghdam, A., Davoody, N., Wright, G., Flowerday, S., & Koch, S. (2020). Effects of electronic health record implementation and barriers to adoption and use: A scoping review and qualitative analysis of the content. *Life (Basel)*, 10(12), Article 327.
<https://doi.org/10.3390/life10120327>

Wibowo, H. P. J., Suliyanto, & Sutrisna, E. (2023). Evaluation of the implementation of the Electronic Medical Record Information (RME) System based on user perceptions using the Technology Acceptance Model (TAM) approach. *International Sustainable Competitiveness Advantage*, 1.

Wijaya, A. P., & Vera, O. (2021). Analisa dan Perencanaan Sistem Informasi Rekam Medis Pada Fasilitas Kesehatan. *Jurnal Ilmiah Infokam*, 17(2), 121-128.

Yeo, L. H., & Banfield, J. (2022). Human factors in electronic health records cybersecurity breach: An exploratory analysis. *Perspect Health Inf Manag*, 19(Spring), 1i.
<https://doi.org/10.35492/PHIM1919>