RAMMIK : Jurnal Rekam Medik dan Manajemen Informasi Kesehatan
Vol. 3, No. 2, Oktober 2024, hlm. 31 - 38
EISSN: 2829-4777
URL : https://rammik.pubmedia.id/index.php/rmik

Keamanan Sistem Informasi Rekam Medis Elektronik di Rumah Sakit Islam Jakarta Sukapura

Endah Wardani[1], Daniel Happy Putra[2], Dina Sonia[3], Noor Yulia[4]

[1,2,3,4]Program Studi Rekam Medis & Informasi Kesehatan, Fakultas Ilmu-Ilmu Kesehatan, Universitas Esa Unggul

endahwardani08@gmail.com, daniel.putra@esaunggul.ac.id, dina.sonia@esaunggul.ac.id, noor.yulia@esaunggul.ac.id

Keywords:

Electronic Medical Record, Information System Security, Hospital

ABSTRACT

The implementation of Electronic Medical Records (EMR) in all health service facilities is outlined in Minister of Health Regulation Number 24 of 2022, with a deadline of 31 December 2023. Ensuring the security of EMR is vital to protect patient data privacy, prevent unauthorized data access, and avoid breaches. This study evaluates the security practices of EMR systems at the Islamic Hospital Jakarta Sukapura using a descriptive qualitative research method with seven informants. The study focuses on six key aspects of EMR security: privacy, integrity, authentication, availability, access control, and non-repudiation. The results show that the hospital has established security procedures, such as using usernames and passwords, but there are significant areas for improvement. The study notes the need for automatic logout features to prevent unauthorized access when computer screens are left unattended and emphasizes the importance of regularly updating passwords to improve security, as well as hospitals using encryption and firewall technologies to protect data during transmission and storage. Apart from this, research shows that some staff members still use default passwords, posing a security risk. Overall, this study provides recommendations for strengthening RME security frameworks in hospitals.

Kata Kunci

Rekam Medis Elektronik, Keamanan Sistem Informasi, Rumah Sakit

ABSTRAK

Penyelenggaraan Rekam Medis Elektronik (RME) di seluruh fasilitas pelayanan kesehatan dituangkan dalam PMK Nomor 24 Tahun 2022, dengan batas waktu 31 Desember 2023. Menjamin keamanan RME sangat penting untuk melindungi privasi data pasien, mencegah akses data yang tidak sah, dan menghindari pelanggaran. Penelitian ini mengevaluasi praktik keamanan sistem RME di RSIJ Sukapura menggunakan metode penelitian deskriptif kualitatif dengan 7 informan. Studi ini berfokus pada 6 aspek utama keamanan RME: privasi, integritas, autentikasi, ketersediaan, kontrol akses, dan tidak ada penolakan. Hasilnya menunjukkan bahwa rumah sakit telah menetapkan prosedur keamanan, seperti penggunaan nama pengguna dan kata sandi, namun masih terdapat beberapa hal yang perlu ditingkatkan. Studi ini memerhatikan perlunya fitur logout otomatis untuk mencegah akses tidak sah ketika layar komputer dibiarkan tanpa pengawasan dan menekankan pentingnya pembaruan kata sandi secara teratur untuk meningkatkan keamanan, serta rumah sakit menggunakan teknologi enkripsi dan firewall untuk melindungi data selama transmisi dan penyimpanan. Selain hal tersebut, penelitian menunjukkan bahwa beberapa anggota staf masih menggunakan kata sandi default, sehingga menimbulkan risiko keamanan. Secara keseluruhan, penelitian ini memberikan rekomendasi untuk memperkuat kerangka keamanan RME di rumah sakit.

Korespondensi Penulis:

Endah Wardani,
Universitas Esa Unggul,
Jl. Arjuna Utara No. 9, Kebon Jeruk, Jakarta Barat
Telepon : +62895323533801
Email: endahwardani08@gmail.com

1. PENDAHULUAN

Rumah Sakit sebagai salah satu jenis fasilitas pelayanan kesehatan perlu menjaga mutu pelayanan medis yang diberikan kepada pasien dan memiliki kewajiban untuk meningkatkan pelayanan yang salah satunya dengan memanfaatkan kemajuan teknologi saat ini [1]. Salah satu bagian yang terdapat dalam SIMRS adalah Rekam Medis Elektronik (RME). Seluruh fasilitas pelayanan kesehatan diwajibkan untuk menyelenggarakan RME dengan batas waktu paling lambat pada tanggal 31 Desember 2023 [2]. RME bertujuan untuk memudahkan akses dan meningkatkan efisiensi pengelolaan informasi kesehatan. Hal ini berpotensi untuk meningkatkan kualitas pelayanan dan mencapai tingkat kesehatan masyarakat yang optimal [3].

Keamanan sistem informasi rekam medis dicantumkan dalam Permenkes No. 24 Tahun 2022, terdapat 3 pasal yang menjelaskan keamanan rekam medis elektronik ialah dari pasal 29 hingga pasal 31. Pasal 29 menegaskan prinsip-prinsip utama yang harus diikuti dalam penyelenggaraan rekam medis elektronik (RME) untuk memastikan keamanan dan perlindungan data, ialah terdapat 3 hal diantaranya kerahasiaan data dan informasi RME, integritas data, dan ketersediaan data RME dapat diakses oleh individu. Pasal 30 memberikan penjelasan lebih lanjut mengenai hak akses yang diberikan kepada tenaga kesehatan dalam mengelola data RME, termasuk penginputan data, perbaikan data, dan melihat data untuk keperluan pelayanan atau administrasi. Pasal 31 memperbolehkan penggunaan tanda tangan elektronik sebagai metode verifikasi dan keamanan dalam memastikan isi RME serta identitas penanda tangan. Penggunaan tanda tangan elektronik harus sesuai dengan ketentuan peraturan perundang-undangan yang berlaku, menjadi salah satu langkah penting dalam pengelolaan data RME di Fasilitas Pelayanan Kesehatan [2].

Keamanan data rekam medis merupakan aspek yang sangat penting serta berbagai upaya dilakukan untuk memastikan bahwa data-data rahasia tersebut tidak dapat diakses oleh individu yang tidak berhak. Jika terjadi pelanggaran keamanan, hal tersebut dapat menimbulkan risiko serius, terutama bagi pasien. Kemungkinan terjadinya akses yang tidak sah dapat mengakibatkan kerugian signifikan. Selain itu, ada juga potensi kerusakan atau kehilangan data jika data tersebut diretas. Perubahan data dalam rekam medis juga dapat mengarah pada kesalahpahaman baik oleh pasien maupun dokter. Oleh karena itu, menjaga keamanan rekam medis menjadi hal yang sangat penting karena rekam medis merupakan data yang bersifat rahasia, sehingga perlu dijaga dengan ketat agar keamanan data rekam medis tetap terjaga [4].

Berdasarkan studi literatur yang dilakukan oleh Siti Sofia terhadap 20 jurnal diketahui dalam menerapkan Rekam Medis Elektronik (RME), terdapat enam aspek keamanan informasi yang harus diperhatikan. Aspek-aspek ini meliputi penggunaan *username* dan *password* yang seringkali rentan jika tidak dikelola dengan baik, kontrol akses yang kurang ketat terutama terkait perubahan atau penghapusan data oleh administrator, penerapan tanda tangan elektronik dan PIN (*Personal Identification Number*) yang belum maksimal, serta strategi backup data yang belum memadai dalam menghadapi risiko peretasan. Selain itu, pembatasan hak akses melalui user ID unik yang tidak selalu diterapkan secara efektif dan pencatatan aktivitas pengguna dalam *log file* yang kurang optimal menambah risiko kebocoran data. Meskipun beberapa fasilitas kesehatan telah mengimplementasikan langkah-langkah ini, standar keamanan sering kali belum terpenuhi sepenuhnya, sehingga diperlukan pengembangan teknik baru atau peningkatan dalam penerapan sistem keamanan untuk melindungi data pasien secara optimal [5].

Rumah Sakit Islam Jakarta Sukapura menjadi salah satu rumah sakit yang telah menerapkan sistem informasi rekam medis elektronik, observasi awal menyatakan aplikasi baru satu tahun digunakan di RSIJ Sukapura. Untuk itu belum mengetahui terkait keamanan-keamanan yang harus diterapkan untuk aplikasi rekam medis elektronik yang digunakan. Berdasarkan uraian tersebut, peneliti ingin mengetahui lebih dalam lagi mengenai "Keamanan Sistem Informasi Rekam Medis Elektronik Di Rumah Sakit Islam Jakarta Sukapura".

2. METODE PENELITIAN

Penelitian ini dilaksanakan di Rumah Sakit Islam Jakarta Sukapura, berlokasi di Jln. Tipar Cakung No. 5 Sukapura, Kecamatan Cilincing, Jakarta Utara, DKI Jakarta, pada periode November 2023 hingga Mei 2024. Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi kasus untuk mengetahui keamanan sistem rekam medis elektronik di RSIJ Sukapura. Subjek penelitian mencakup 4 perekam medis dan informasi kesehatan, 3 petugas *Information & Technology* (IT), serta petugas keteknisian aplikasi Zi-Care, sementara objek penelitian adalah aplikasi Zi-Care yang digunakan untuk mengelola rekam medis elektronik. Variabel penelitian mencakup identifikasi Standar Prosedur Operasional (SPO) dan teknis penyelenggaraan rekam medis elektronik, serta identifikasi keamanan rekam medis yang diterapkan oleh rumah sakit. Teknik pengumpulan data meliputi observasi menggunakan instrumen berupa daftar tilik (forumulir *checklist*), wawancara terstruktur kepada petugas terkait dengan menggunakan pedoman wawancara, dan studi literatur dari berbagai sumber seperti jurnal, artikel, dan penelitian sebelumnya. Analisis data dilakukan menggunakan pendekatan deskriptif kualitatif, dengan pemaparan kondisi sebenarnya yang dibandingkan dengan teori-teori terkait, serta kesimpulan yang diperoleh melalui uji analisis dengan aplikasi Nvivo.

3. HASIL DAN ANALISIS

3.1 Hasil Identifikasi Standar Prosedur Operasional dan Tehnis Penyelenggaraan Rekam Medis Elektronik di Rumah Sakit Islam Jakarta Sukapura

Implementasi rekam medis elektronik baru dijalankan dalam kurun waktu satu tahun oleh RSIJ Sukapura, terhitung sejak awal tahun 2023. Penggunaan rekam medis elektornik ini terbilang masih baru, tentunya keamanan dari rekam medis elektronik belum di perhatikan secara khusus oleh RSIJ Sukapura. Saat ini, RSIJ Sukapura belum memiliki kebijakan tambahan terkait perlindungan rekam medis elektronik dari akses tidak sah. Standar Prosedur Operasional (SPO) Nomor 33 terkait Perlindungan Rekam Medis Dari Penggunaan / Akses Tidak Sah, masih menggabungkan perlindungan rekam medis manual dan elektronik dalam satu kebijakan, sehingga kebutuhan keamanan khusus untuk rekam medis elektronik belum terakomodasi secara memadai. Untuk mengatasi kekurangan ini, sangat penting bagi RSIJ Sukapura untuk segera memisahkan SPO terkait keamanan rekam medis elektronik dari manual, serta mengembangkan kebijakan tambahan yang relevan.

Keamanan rekam medis elektronik dijelaskan dari poin ke-4 sampai dengan ke-7 yang berisikan sebagai berikut, 4) Akses terhadap komputer program rekam medis harus melalui *username* dan *password* yang telah disediakan bagi masing-masing petugas sesuai batasan kewenangan masing-masing. 5) Masing-masing petugas yang memiliki hak akses untuk mengakses program rekam medis harus mampu menajaga *username* dan *password* masing-masing agar tidak dapat diketahui petugas / pihak lain yang tidak bertanggung jawab. 6) Tiap petugas yang mengakses program rekam medis harus login menggunakan *username* dan *password* masing-masing terlebih dahulu untuk dapat mengakses program rekam medis dan harus segera *logout* jika sudah tidak menggunakan aplikasi program rekam medis. 7) *Password* harus segera diganti secara berkala untuk menghindari akses dari pihak yang tidak bertanggung jawab.

Hasil penelitian di RSIJ Sukapura didapatkan, setiap petugas sudah mengikuti aturan SPO ke-4 dan ke-6 dimana untuk mengkases Aplikasi Zi-Care perlu memasukkan *username* dan *password*, setiap petugas memiliki akunnya masing-masing untuk melakukan *login* aplikasi dan semua petugas mengikuti arahan dengan melakukan *logout* manual saat setelah digunakan. Pada SPO ke-5 terkait "masing-masing petugas yang memiliki hak akses untuk mengakses program rekam medis harus mampu menajaga *username* dan *password* masing-masing agar tidak dapat diketahui petugas / pihak lain yang tidak bertanggung jawab", terdapat ketidaksesuaian dengan temuan dari peneliti karena peneliti menemukan adanya petugas yang menyimpan akunnya didalam *browser*, dimana seharusnya hal ini tidak boleh dilakukan karena berpotensi disalahgunakan oleh pihak yang tidak bertanggung jawab.

Penyimpanan *username* dan *password* didalam browser tentunya tidak boleh dilakukan, karena hal ini akan akan berdampak buruk terhadap data-data yang berkaitan dengan akun tersebut dan memungkinkan adanya kebocoran data. Hal ini rentan terhadap serangan pencurian *password* (*password stealing attack*). Dalam serangan pencurian *password*, penyerang menggunakan teknik untuk mengambil *file saved password* dengan menggunakan perangkat lunak berbahaya (*malicious software / malware*) untuk mendapatkan akses yang tidak sah ke akun korban. Beberapa cara yang dapat digunakan oleh penyerang yaitu dengan menggunakan *Microcontroller Universal Serial Bu*s (USB), sebagai USB *flashdrive* dapat

mendaftarkan dirinya sebagai perangkat lain seperti keyboard sehingga memungkinkan USB tersebut dapat menjalankan *script* berbahaya. Cara lainnya ialah dengan *Phishing Attack*, yaitu penyerang membuat situs web palsu yang menyerupai situs asli untuk mencuri informasi penting korban [6].

SPO ke-7 terkait "*Password* harus segera diganti secara berkala untuk menghindari akses dari pihak yang tidak bertanggung jawab", peneliti mendapatkan temuan bahwa masih adanya petugas yang menggunakan *password default* (*password* yang diberikan sejak awal penggunaan), dimana hal seperti ini seharusnya tidak boleh karena *password* seperti itu mudah diketahui oleh petugas lainnya dan memungkinkan adaya akses tidak sah yang dilakukan oleh pihak yang tidak bertanggung jawab.

3.2 Hasil Identifikasi Keamanan yang dilakukan oleh Rumah Sakit Islam Jakarta Sukapura terhadap Rekam Medis Elektronik

Penelitian yang dilakukan oleh Siti Sofia, mengatakan terdapat 6 aspek yang harus diterapkan sebagai bentuk keamanan rekam medis elektronik, yaitu Aspek Privasi, Aspek Integritas, Aspek Autentikasi, Aspek Ketersediaan, Aspek Kontrol Akses, dan Aspek Tidak Ada Penolakan [5]. Hasil penelitian yang dilakukan oleh peneliti terhadap Aplikasi Zi-Care mengenai 6 aspek tersebut ialah :

1) Aspek Privasi

Penggunaan *username* dan *password*, fitur otomatis *logout* dan penggunaan teknologi *enkripsi* maupun pemblokiran diterapkan sebagai aspek privasi. RSIJ Sukapura menerapkan penggunaan *username* dan *password* bagi petugas yang memiliki akses untuk masuk kedalam Aplikasi Zi-Care. Penggunaan *username* dan *password* untuk masuk kedalam sebuah aplikasi tentunya diperlukan, karena *username* dan *password* digunakan sebagai bukti bahwa pengguna memiliki wewenang untuk menggunakan dan mengakses sistem. Hal ini sebagai bentuk pentingnya penggunaan *username* dan *password* untuk mengkases ke rekam medis elektronik serta ditekankan sebagai langkah kunci dalam memastikan keamanan dan privasi informasi pasien [7].

Langkah selanjutnya yaitu dengan tersedianya fitur otomatis pada aplikasi, namun hasil pengamatan diketahui Aplikasi Zi-Care tidak memiliki fitur tersebut, sehingga setiap petugas yang telah selesai menggunakan aplikasi diharapkan melakukan *logout* sendiri agar akun nya tidak disalahgunakan. Hal ini Ini sangat penting untuk mencegah akses yang tidak sah jika pengguna meninggalkan komputer dalam waktu yang cukup lama. Aspek privasi dapat dijaga dengan mengimplementasikan fitur *logout* otomatis dalam sistem informasi. Langkah ini bertujuan sebagai bentuk pertahanan dan pencegahan terhadap penyalahgunaan *user identification* [5].

Penggunakan teknologi enkripsi dan pemblokiran melalui jaringan wifi juga perlu dilakukan untuk menghindari adanya peretasan yang dilakukan oleh pihak yang tidak bertanggung jawab untuk memperoleh informasi atau data-data yang penting. Serangan di dunia maya bisa menyerang jaringan komputer, menyusup, mencuri data rahasia, dan merusak sistem jaringan. Untuk mengatasi ancaman ini, diperlukan sistem yang dilengkapi dengan *firewall*. *Firewall* digunakan sebagai fitur keamanan jaringan yang bertugas untuk melindungi server, jaringan, dan mencegah serangan - serangan yang mencoba merusaknya [8]. RSIJ Sukapura menerapkan metode *firewall* yang digunakan pada jaringan Wi-Fi dan dipantau oleh sebuah aplikasi sebagai bentuk pencegahan terhadap ancaman luar, yaitu dengan menggunakan *Web Application Firewall* (WAF).

Penggunaan *username* dan *password* di aplikasi Zi-Care adalah langkah penting untuk keamanan informasi pasien, tetapi terdapat kekurangan, seperti tidak adanya fitur otomatis logout yang meningkatkan risiko penyalahgunaan akun. Meskipun teknologi enkripsi, pemblokiran, dan penggunaan *Web Application Firewall* (WAF) sudah diterapkan, perlu ada jaminan bahwa langkah-langkah tersebut berfungsi optimal untuk melindungi sistem dari serangan dalam jaringan. Oleh karena itu, implementasi fitur logout otomatis dan pengawasan keamanan sangat penting untuk meningkatkan privasi dan perlindungan data pasien di RSIJ Sukapura.

2) Aspek Integritas

Aspek integritas adalah faktor yang terkait dengan penghapusan dan perubahan data, di mana semua perubahan pada sistem atau rekam medis elektronik dapat dideteksi oleh sistem. Sedangkan, penghapusan data pada rekam medis elektronik tidak memungkinkan dilakukan, oleh karena itu perlindungan yang lebih kuat harus diperlukan, di mana data tidak dapat dihapus secara langsung dan semua perubahan yang terdapat pada data dapat terlacak [5]. Di RSIJ Sukapura, dokter atau tenaga kesehatan lainnya yang ingin melakukan perubahan pada data medis pasien, perlu mengajukan MoM (*Minute of Meeting*) atas persetujuan dari kepala rekam medis. Perubahan data medis tidak tercatat pada sistem

Aplikasi Zi-Care, semua perubahan data medis yang dilakukan riwayatnya hanya terdapat pada lembar permohonan perubahan (MoM). Dengan adanya persetujuan dari pihak rekam medis dan tersimpannya dokumen MoM akan menjamin keamanan dari rekam medis pasien.

Rumah sakit telah menetapkan prosedur yang baik pada sistem untuk mendeteksi perubahan data melalui pengajuan MoM (*Minute of Meeting*), namun masih ada kekurangan dalam pencatatan perubahan tersebut. Perubahan yang dilakukan tidak tercatat dalam sistem Aplikasi Zi-Care, melainkan hanya terdapat pada dokumen permohonan perubahan. Meskipun persetujuan dari pihak rekam medis dan penyimpanan dokumen MoM menjamin keamanan data, adanya ketidakjelasan dalam pencatatan perubahan ini dapat mengurangi transparansi dan akuntabilitas. Oleh karena itu, diperlukan peningkatan dalam sistem pencatatan perubahan data agar semua riwayat perubahan dapat terlacak secara digital untuk meningkatkan integritas dan keamanan rekam medis pasien.

3) Aspek Autentikasi

Penggunaan tanda tangan digital dalam rekam medis elektronik berperan sebagai alat untuk autentikasi dan verifikasi identitas penandatanganan, serta memastikan integritas dan keaslian informasi elektronik. Tanda tangan digital akan beresiko jika digunakan tanpa pihak ketiga sebagai penjamin, ada risiko manipulasi oleh pihak yang tidak bertanggung jawab jika *password* akun untuk tanda tangan digital tersebut bocor. Meskipun tanda tangan digital merupakan inovasi teknologi yang mendukung tujuan tersebut, tantangan dalam implementasinya adalah bagaimana membatasi akses dan mencegah kebocoran *password* oleh pengguna. Kesadaran akan pentingnya keamanan informasi dalam sistem informasi menjadi kunci dalam mengatasi tantangan ini [9]. Hal itupun yang dilakukan oleh RSIJ Sukapura yang menggunakan tanda tangan digital dengan bentuk tanda tangan yang dibuat melalui alat perekam tanda tangan dan kemudian disimpan di akun masing-masing pengguna.

Penggunaan tanda tangan digital di RSIJ Sukapura menunjukkan bahwa meskipun tanda tangan digital berfungsi efektif untuk autentikasi, verifikasi identitas, dan memastikan integritas informasi elektronik, terdapat risiko yang perlu diperhatikan. Tanda tangan digital berpotensi rentan terhadap manipulasi jika tidak ada pihak ketiga sebagai penjamin dan jika *password* akun tersebar. Kesadaran pengguna akan pentingnya perlindungan informasi tetap menjadi kunci untuk mengatasi risiko dan memastikan keandalan penggunaan tanda tangan digital dalam rekam medis elektronik.

4) Aspek Ketersediaan

Aspek ketersediaan pada sistem atau aplikasi kesehatan yaitu dengan terintegrasinya antara aplikasi dengan BPJS Kesehatan dan Satu Sehat. Aplikasi Zi-Care yang diterapkan oleh RSIJ Sukapura telah terintegrasi dengan BPJS Kesehatan. Dengan integrasi yang luas dari Sistem Informasi Manajemen Rumah Sakit (SIMRS), proses pelayanan di rumah sakit akan menjadi lebih efisien dan lancar [10]. Aplikasi Zi-Care belum sepenuhnya terintegrasi dengan Satu Sehat, sampai saat ini Aplikasi Zi-Care masih berada di fase kedua dari lima fase untuk mencapai proses integrasi sepenuhnya dengan Satu Sehat.

Aplikasi Satu Sehat adalah sebuah platform yang menghubungkan sistem untuk mengintegrasikan data kesehatan individu antara berbagai fasilitas kesehatan. Di masa mendatang, pasien akan memiliki akses untuk melihat rekam medis atau riwayat perjalanan keseheta mereka melalui aplikasi Satu Sehat, yang sesuai dengan program Kementerian Kesehatan [11]. Untuk itu aplikasi harus melanjutkan proses untuk ke Satu Sehat karena nantinya berguna bagi pasien.

Penggunaan rekam medis elektronik di rumah sakit harus didukung oleh server yang handal. Server ini adalah sistem komputer yang menyediakan layanan spesifik dalam hal penyimpanan data. Berbagai jenis dokumen disimpan dalam server ini dan informasi diberikan kepada pengguna atau pengunjung. Peran utama dari server adalah memenuhi semua permintaan pemrosesan dari klien, termasuk permintaan data atau aplikasi yang dilakukan oleh klien [12]. RSIJ Sukapura menyediakan server aplikasi dan server database pada Aplikasi Zi-Care guna menunjang segala kebutuhan.

Aplikasi Zi-Care di RSIJ Sukapura menunjukkan bahwa integrasi aplikasi dengan BPJS Kesehatan telah berhasil dilakukan, sehingga meningkatkan efisiensi dan kelancaran proses pelayanan di rumah sakit. Namun, aplikasi ini masih belum sepenuhnya terintegrasi dengan Satu Sehat, yang saat ini berada di fase kedua dari lima fase integrasi. Integrasi penuh dengan Satu Sehat sangat penting, karena akan memberikan pasien akses untuk melihat rekam medis dan riwayat kesehatan mereka di masa depan, sejalan dengan program Kementerian Kesehatan. Oleh karena itu, melanjutkan proses integrasi ke Satu Sehat adalah langkah penting untuk mendukung kebutuhan pasien. Selain itu, penyediaan server aplikasi dan database yang handal di RSIJ Sukapura menjadi kunci dalam mendukung ketersediaan dan keamanan data dalam sistem rekam medis elektronik.

5) Aspek Kontrol Akses

Keamanan data pasien merupakan prioritas utama bagi sistem layanan kesehatan, terutama terkait dengan data sensitif seperti Rekam Medis Elektronik. Pengendalian akses menjadi kunci untuk memastikan keamanan ini. Kontrol akses yang efektif memastikan bahwa data kesehatan sensitif hanya dapat diakses oleh pihak yang berwenang, sehingga mengurangi kemungkinan akses yang tidak sah. Kontrol akses yang aman sangat penting dalam mencegah pelanggaran data dengan mengatur akses ke data pasien yang sensitif. Pendekatan ini secara efektif mengurangi risiko pencurian data, serangan siber, dan ancaman keamanan lainnya. Selain itu, kontrol akses yang aman juga memastikan bahwa hanya individu yang berhak yang dapat mengakses informasi sensitif pasien [13].

Penerapan kontrol akses pada Aplikasi Zi-Care akan memudahkan RSIJ Sukapura untuk melakukan audit trail yang umumnya digunakan untuk melakukan investigasi jika terjadinya kebocoran data dari sistem Aplikasi Zi-Care. Aplikasi Zi-Care yang digunakan oleh RSIJ Sukapura menerapkan hak akses yang berbeda-beda bagi setiap petugas dalam menjaga keamanan dari rekam medis elektronik. Penerapan kontrol akses yang aman sangat penting dalam mencegah pelanggaran data, yang dapat merugikan dan merugikan organisasi layanan kesehatan. Dengan membatasi akses terhadap data sensitif, kemungkinan pelanggaran data dapat diminimalkan secara signifikan [13].

RSIJ Sukapura mengutamakan pentingnya kontrol akses yang efektif dalam melindungi data sensitif seperti Rekam Medis Elektronik. Dengan menerapkan hak akses yang berbeda untuk setiap petugas untuk mengakses sistem ini dapat mengurangi risiko akses tidak sah dan pelanggaran data. Kontrol akses yang aman juga memungkinkan audit trail untuk investigasi jika terjadi kebocoran data. Meskipun langkah-langkah ini sudah baik, pemantauan dan evaluasi berkala tetap diperlukan untuk memastikan efektivitasnya dalam menjaga integritas dan keamanan informasi pasien.

6) Tidak Ada Penolakan

Tersedianya riwayat untuk melihat jejak pengisian data dan mengidentifikasi siapa yang bertanggung jawab atas perubahan data diperlukan pada sebuah sistem di fasilitas kesehatan. Hasil penelitian terhadap Aplikasi Zi-Care yang digunakan di RSIJ Sukapura belum optimal, sistem tidak dapat mengidentifikasi pengguna yang melakukan modifikasi pada informasi pasien dalam rekam medis elektronik (RME), sistem hanya dapat menampilkan data terbaru.

Log audit merupakan dokumentasi terperinci mengenai aktivitas pengguna dalam sistem, yang mencakup identitas pengguna yang mengakses data, waktu akses, dan kegiatan yang dilakukan terhadap data tersebut. Catatan ini menyajikan detail tentang akses, seperti pengguna yang terlibat, subjek data (misalnya, pasien), tindakan yang dilakukan (seperti melihat laporan), dan waktu kejadian. Ketidakmampuan aplikasi untuk melihat rekam jejak data perubahan akan berpotensi membuat pengguna atau individu menyangkal keterlibatannya dalam transaksi pada sistem elektronik tersebut. Konsekuensinya, kesulitan dalam melacak sejarah perubahan data pasien, potensi penyalahgunaan data pasien, dan risiko kemungkinan penyangkalan keterlibatan oleh pengguna atau individu [5] [14].

Sistem Aplikasi Zi-Care di RSIJ Sukapura menunjukkan bahwa meskipun penting untuk memiliki riwayat pengisian data dan identifikasi pengguna yang melakukan perubahan, aplikasi saat ini belum mampu melakukan hal tersebut secara optimal. Sistem hanya menampilkan data terbaru tanpa log audit yang mencatat aktivitas pengguna, waktu akses, dan tindakan yang dilakukan. Akibatnya, hal ini menghambat kemampuan untuk melacak perubahan data pasien, meningkatkan risiko penyalahgunaan, dan mempersulit dalam pengawasan. Oleh karena itu, diperlukan peningkatan dalam pelacakan jejak perubahan untuk memperkuat integritas dan keamanan data pasien.

4. KESIMPULAN

4.1 Kesimpulan

1. Rumah Sakit Islam Jakarta Sukapura belum sepenuhnya memiliki Standar Prosedur Operasional (SPO) khusus untuk mengatur keamanan sistem informasi rekam medis elektronik. Meskipun terdapat SPO Nomor 33 yang mengenai Perlindungan Rekam Medis Dari Penggunaan/Akses Tidak Sah, terdapat ketidaksesuaian antara isi SPO dan praktik di lapangan. Beberapa poin, seperti poin 5 dan 7, menunjukkan adanya kekurangan dalam menjaga keamanan sistem, seperti penyimpanan *username* dan *password* di *browser* dan penggunaan *password default* oleh beberapa petugas. Hal ini dapat disimpulkan bahwa SPO yang dimiliki oleh RSIJ Sukapura belum terlaksana dengan baik dalam praktiknya.

2. Aplikasi Zi-Care sebagai sistem informasi rekam medis elektronik di RSIJ Sukapura telah memenuhi beberapa aspek keamanan, seperti Integritas, Autentikasi, dan Kontrol Akses, namun terdapat tiga aspek keamanan yang belum terlaksana dengan baik, yaitu Aspek Privasi (fitur otomatis *logout*), Aspek Ketersediaan (ketersambungan dengan Satu Sehat), dan Aspek Tidak Ada Penolakan (riwayat perubahan data) adalah hal-hal yang perlu diperbaiki dalam aplikasi tersebut. Dengan demikian, dapat disimpulkan bahwa Aplikasi Zi-Care belum memenuhi standar keamanan yang seharusnya ada dalam sistem informasi kesehatan.

4.2 Saran

1. Untuk SPO Nomor 33 disarankan perlu adanya penambahan larangan terhadap penyimpnan *username* dan *password* di dalam *browser* dan disarankan agar Unit Rekam Medis berkoordinasi dengan pihak IT untuk menetapkan peraturan mengenai batas waktu penggunaan *password*, dengan mengatur periode *expired password* dalam rentang waktu 3 hingga 6 bulan. Langkah tambahan yang dapat diterapkan adalah Autentikasi Dua Faktor (2FA), dimana pengguna diharuskan memasukkan kode yang dikirimkan melalui SMS atau aplikasi autentikator. Hal ini diharapkan dapat meningkatkan keamanan sistem informasi rekam medis elektronik di RSIJ Sukapura.
2. Sedangkan untuk Aplikasi Zi-Care disarankan Aplikasi Zi-Care perlu melakukan pembaruan (*update*) untuk memperbaiki keamanan rekam medis elektronik. Pembaruan tersebut meliputi penyediaan fitur *logout* otomatis, penyediaan riwayat perubahan data pasien yang dapat dilacak dalam sistem, dan menyelesaikan tahapan integrasi dengan Satu Sehat untuk mempermudah pasien dalam melihat riwayat pengobatannya. Hal ini diharapkan dapat meningkatkan keamanan dan kualitas layanan sistem informasi rekam medis elektronik yang digunakan oleh Rumah Sakit Islam Jakarta Sukapura.

UCAPAN TERIMA KASIH

Terimakasih kepada Bapak Daniel Happy Putra selaku ketua Program Studi Rekam Medis dan Informasi Kesehatan Fakultas Ilmu-Ilmu Kesehatan Universitas Esa Unggul, sebagai Dosen Pembimbing Akademik yang selalu memberikan masukan selama menjalankan program studi D-III, dan sebagai Dosen Pembimbing KTI yang senantiasa membimbing dan mengarahkan penulis dalam menyelesaikan Karya Tulis Ilmiah ini. Terimakasih juga kepada keluarga dan teman-teman saya yang senantiasa mendukung saya untuk proses penyelesaian tugas akhir.

REFERENSI

[1] Kemenkes RI, "Peraturan Menteri Kesehatan Republik Indonesia Nomor 82 Tahun 2013 Tentang Sistem Informasi Manajemen Rumah Sakit." p. 2, 2013.
[2] Kemenkes RI, "Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 Tentang Rekam Medis." p. 3, 2022.
[3] M. K. Maha Wirajaya and N. M. U. K. Dewi, "Analisis Kesiapan Rumah Sakit Dharma Kerti Tabanan Menerapkan Rekam Medis Elektronik," *J. Kesehat. Vokasional*, vol. 5, no. 1, p. 1, 2020, doi: 10.22146/jkesvo.53017.
[4] P. H. Yosi Tanjung, "Penerapan Algoritma Aes 625 Dalam Pengamanan Data Rekam Medis," *J. Glob. Tecnol. Comput.*, vol. 1, no. 3, pp. 77–83, 2022.
[5] S. Sofia, E. T. Ardianto, N. Muna, and S. Sabran, "Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Fasilitas Kesehatan," *J. Rekam Med. Manaj. Inf. Kesehat.*, vol. 1, no. 2, pp. 94–103, 2022, doi: 10.47134/rmik.v1i2.29.
[6] F. Akram, "Implementasi Password Stealing Attack Terhadap Saved Password Pada Browser Komputer Menggunakan Digispark Attiny85," *J. Ilm. Kriptologi*, vol. 17, no. 1, pp. 7–14, 2023, doi: 10.56706/ik.v17i1.69.
[7] A. We'e, R. H. Nugroho, and H. Siswatibudi, "Evaluasi Aspek Keamanan Dan Kerahasiaan Rekam Medis Elektronik Di Rumah Sakit Panti Nugroho," *J. Permata Indones.*, vol. 14, no. 2, pp. 72–81, 2023, doi: 10.59737/jpi.v14i2.265.
[8] A. S. Wahyusesa, P. W. Hidayanto, and E. A. Ramdayani, "Solusi Cerdas: Meningkatkan Keamanan dan Kinerja Jaringan pada Warnet dengan Mengatasi Kelemahan Sistem," *J. Ilmu Multidisiplin*, vol. 1, no. 2, pp. 62–66, 2023, [Online]. Available: https://ejournal.cvrobema.com/index.php/dike/article/view/39.
[9] H. Putri, M. R. Anshari, and G. Persadha, "Persiapan Implementasi Tanda Tangan Digitak Untuk Autentikasi Dokumen Rekam Medis Elektronik Di RSUD dr. H. Moch Ansari Saleh Banjarmasin," *J. Kaji. Ilm. Kesehat. Dan Teknol.*, vol. 5, no. 2, pp. 64–70, 2023, [Online]. Available: https://jurnal.polanka.ac.id/index.php/JKIKT/article/view/112.
[10] T. Rahmaddian and L. Faaghna, "Evaluasi Implementasi Sistem Informasi Manajemen Rumah Sakit

(SIMRS) Rekam Medis dengan Metode Problem Solving Tools di Rumah Sakit X," *J. Kesehat.*, vol. 12, no. 2, pp. 339–345, 2023, doi: 10.46815/jk.v12i2.176.

[11] R. N. Belrado, Harmendo, and S. Wahab, "Analisis Penggunaan Rekam Medis Elektronik Di Rumah Sakit," *J. Penelit. Perawat Prof.*, vol. 6, no. 5474, pp. 1779–1798, 2024, [Online]. Available: https://www.jurnal.globalhealthsciencegroup.com/index.php/JPPP/article/view/3039.

[12] B. Wahab, A. Sembiring, A. Apriana, and Efrata, "Pendampingan Digitalisasi Berkas Rekam Medis Guna Mendukung Keberhasilan Implementasi Rekam Medis Elektronik Di RSUP Haji Adamalik Medan," *J. Pengabdi. Masy. Putri Hijau*, vol. 4, no. 2, pp. 79–83, 2024, [Online]. Available: http://ejournal.delihusada.ac.id/index.php/JPMPH/article/view/1712.

[13] P. Shojaei, E. Vlahu-Gjorgievska, and Y. W. Chow, "Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review," *Computers*, vol. 13, no. 2, 2024, doi: 10.3390/computers13020041.

[14] M. Hedda, B. A. Malin, C. Yan, and D. Fabbri, "Evaluating the Effectiveness of Auditing Rules for Electronic Health Record Systems," *Natl. Cent. Biotechnol. Inf.*, pp. 866–875, 2018, [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5977720/.