KOLONI: Jurnal Multidisiplin Ilmu, 5(2), Tahun 2026
e-ISSN: 2828-6863

Tinjauan Aspek Keamanan Informasi Data Pasien dalam Penerapan RME Di RSUP dr. Sitanala

Sela Abdiyana[1*], Dina Sonia[2], Noerfitri[3], Bangga Agung Satrya[4]
[1]Program Studi Rekam Medis dan Informasi Kesehatan, Universitas Esa Unggul, Indonesia
[2,3,4]Program Studi Rekam Medis dan Informasi Kesehatan, Universitas Esa Unggul, Indonesia
sellaapdiana@gmail.com

Abstrak: Penerapan RME merupakan bagian dari transformasi digital pelayanan kesehatan yang bertujuan meningkatkan mutu pelayanan, efisiensi, serta akurasi pengelolaan data pasien. Namun, digitalisasi tersebut juga menimbulkan tantangan dalam menjaga keamanan informasi yang bersifat sensitif, sehingga diperlukan perlindungan terhadap kerahasiaan, keutuhan, dan ketersediaan data. Penelitian ini bertujuan untuk meninjau penerapan aspek keamanan informasi data pasien dalam sistem Rekam Medis Elektronik (RME) di RSUP Dr. Sitanala. Penelitian ini menggunakan metode deskriptif dengan pendekatan kualitatif. Pengumpulan data dilakukan melalui observasi dan wawancara mendalam terhadap delapan informan yang terdiri dari kepala rekam medis, dokter, perawat, kepala IT, dan petugas IT. Analisis difokuskan pada enam aspek keamanan informasi, yaitu privacy, integrity, authentication, availability, access control, dan non-repudiation. Hasil penelitian menunjukkan bahwa penerapan keamanan informasi dalam sistem RME secara umum telah berjalan cukup baik. Aspek privacy dan access control diterapkan melalui penggunaan akun individual dan pembatasan hak akses sesuai peran. Aspek integrity dijaga melalui pembatasan kewenangan perubahan data, sedangkan authentication dilakukan melalui mekanisme login berbasis username dan password. Aspek availability didukung oleh ketersediaan sistem dan proses pencadangan data, serta non-repudiation melalui pencatatan aktivitas pengguna dalam log sistem. Meskipun demikian, masih ditemukan kelemahan pada penerapan log-out otomatis yang belum optimal, sehingga berpotensi menimbulkan risiko keamanan. Oleh karena itu, diperlukan evaluasi dan peningkatan berkelanjutan guna mengoptimalkan perlindungan data pasien serta menjaga kepercayaan masyarakat terhadap pelayanan kesehatan.

Kata kunci: rekam medis elektronik; keamanan informasi; data pasien

Abstract: *The implementation of EMR is part of the digital transformation of healthcare services aimed at improving service quality, efficiency, and accuracy of patient data management. However, this digitalization also poses challenges in maintaining the security of sensitive information, necessitating protection of data confidentiality, integrity, and availability. This study aims to review the implementation of patient data information security aspects in the Electronic Medical Records (EMR) system at Dr. Sitanala General Hospital. This research employed a descriptive method with a qualitative approach, collecting data through observation and in-depth interviews with eight informants, including the head of medical records, doctors, nurses, the head of IT, and IT staff. The analysis focused on six aspects of information security: privacy, integrity, authentication, availability, access control, and non-repudiation. The findings indicate that information security within the EMR system has generally been implemented adequately, with privacy and access control ensured through individual user accounts and role-based access restrictions, integrity maintained by limiting data modification authority, authentication conducted via username and password-based login mechanisms, availability supported by system reliability and data backup processes, and non-repudiation ensured through user activity logs. Nevertheless, weaknesses were identified in the automatic log-out feature, which has not yet functioned optimally and may pose potential security risks, highlighting the need for continuous evaluation and improvement to strengthen patient data protection and maintain public trust in healthcare services.*

Keywords*: electronic medical records; information security; patient data*

Pendahuluan

Rumah sakit merupakan salah satu sarana pelayanan kesehatan milik swasta atau pemerintah. Rumah sakit mempunyai tanggung jawab untuk menyediakan perawatan kesehatan komprehensif bagi masyarakat, meliputi perawatan preventif, kuratif, dan rehabilitatif serta

pelayanan rawat inap, rawat jalan dan gawat darurat (Kemenkes RI, 2020). Rumah Sakit, sebagai institusi yang menyelenggarakan pelayanan kesehatan, berperan penting dalam memastikan dan meningkatkan standar mutu pelayanan kesehatan. Peran penting ini harus diimbagi dengan standar kualitas pelayanan di rumah sakit (Christianto & Dewi, 2022).

Rekam medis elektronik (RME) merupakan rekam medis yang dibuat dengan menggunakan sistem elektronik (Permenkes No. 24, 2022). Rekam medis elektronik diselenggarakan guna untuk mencapai penyelenggaraan pelayanan kesehatan yang cepat, tepat, dan akurat. Setiap kemudahan dan manfaat yang dihasilkan dari penerapan rekam medis elektronik tidak terlepas dari ancaman yang harus diantisipasi oleh setiap fasilitas pelayanan kesehatan (Ardianto et al., 2024). Salah satu permasalahan utama jika dikaitkan dengan perkembangan teknologi informasi adalah masalah keamanan data.

Kerahasiaan, integritas, dan ketersediaan data pasien dari sumber internal maupun eksternal. Aspek ini krusial untuk melindungi privasi pasien, mencegah kehilangan data, dan memastikan bahwa hanya individu yang berwenang yang dapat mengakses data. Dalam konteks RME, ancaman keamanan seperti tidak sah akses, peretasan, dan kehilangan data dapat berdampak signifikan terhadap kepercayaan publik terhadap puskesmas (Himastuti et al., 2023)

Semua fasilitas kesehatan wajib menyelenggarakan RME untuk meningkatkan kualitas pelayanan (Permenkes No. 24, 2022). Namun, penerapan ini juga meningkatkan risiko terhadap keamanan data dan kerahasiaan informasi pasien, mengingat data pasien merupakan aset yang sangat sensitif dan harus dijaga integritas, kerahasiaan, serta ketersediaannya. RME memiliki dampak positif yang besar dalam mengakses informasi klinis, namun aspek keamanan menjadi salah satu perhatian utama, terutama dalam menjaga kerahasiaan dan keamanan data pasien (Tiorentap, 2020). Penerapan standar keamanan yang memadai menjadi keharusan untuk mencegah risiko-risiko seperti akses tidak sah, modifikasi data, dan pencurian informasi.

Menurut penelitian di Puskesmas Botania menunjukkan bahwa penerapan RME masih menghadapi masalah keamanan data pasien. Sistem e-Puskesmas belum sepenuhnya menjaga kerahasiaan, keutuhan, dan ketersediaan data. Penggunaan akun bersama memungkinkan akses oleh pihak tidak berwenang, sehingga berisiko melanggar privasi. Selain itu, pengelolaan perubahan data belum efisien dan sistem belum terintegrasi dengan BPJS *Health*, yang menghambat proses klaim. Penelitian ini merekomendasikan penggunaan akun individual, *log out* otomatis, enkripsi, pembatasan akses, serta integrasi sistem, disertai peningkatan teknologi dan SDM agar RME lebih aman dan efektif (Pradita et al., 2022).

Penelitian ini dilakukan di Rumah Sakit Umum Pusat Dr. Sitanala yang merupakan rumah sakit vertikal milik Kementerian Kesehatan Republik Indonesia dengan klasifikasi Kelas A, beralamat di Jl. DR. Sitanala No.99, RT.002/RW.003, Karang Sari, Kec. Neglasari, Kota Tangerang, Banten 1512. Rumah sakit tersebut telah menerapkan aplikasi Sistem Informasi Manajemen Rumah Sakit

(SIMRS) GOS dalam operasionalnya sejak tahun 2014.Hasil observasi awal, diketahui bahwa penerapan sistem keamanan dan kerahasiaan data pasien pada RME di RSUP Dr. Sitanala telah dijalankan. Namun, pada tahun 2024, rumah sakit ini sempat mengalami insiden serangan siber yang berlangsung kurang lebih 3 jam, menyebabkan gangguan *(downtime)* pada sistem pendaftaran *online,* sehingga proses pelayanan pasien sempat terhambat. Selain itu, aplikasi SIMRS GOS untuk pengguna *log-out* otomatis dapat terjadi setelah 2 jam aplikasi tersebut tidak digunakan. Sementara standarnya untuk keamanan sistem, aplikasi itu harus dapat *log-out* otomatis setelah 5 – 15 menit (Melisa et al., 2024). Penelitian ini bertujuan untuk meninjau aspek keamanan informasi data pasien dalam penerapan RME di RSUP Dr. Sitanala.

Metode

Penelitian ini menggunakan desain penelitian deskriptif dengan pendekatan kualitatif untuk menggambarkan penerapan aspek keamanan informasi data pasien pada sistem RME di RSUP Dr. Sitanala. Penelitian dilaksanakan di RSUP Dr. Sitanala Kota Tangerang pada periode September 2025 sampai Januari 2026. Populasi penelitian adalah seluruh pengguna sistem RME yang terlibat dalam pengelolaan dan pemanfaatan data pasien di RSUP Dr. Sitanala. Sampel penelitian menggunakan teknik purposive sampling sebanyak 8 informan, terdiri dari 1 kepala rekam medis, 2 dokter, 2 perawat, 1 kepala IT, dan 2 petugas IT.

Pengumpulan data dilakukan melalui observasi langsung terhadap penggunaan sistem RME serta wawancara mendalam menggunakan pedoman wawancara terstruktur. Data yang dikumpulkan difokuskan pada enam aspek keamanan informasi, yaitu *privacy, integrity, authentication, availability, access control,* dan *non-repudiation*. Analisis data dilakukan secara deskriptif kualitatif melalui tahapan reduksi data, penyajian data, dan penarikan kesimpulan. Keabsahan data diuji menggunakan triangulasi sumber dengan membandingkan informasi antar informan serta triangulasi metode melalui hasil observasi dan wawancara.

Hasil dan Pembahasan

Penerapan *privacy* di RSUP dr. Sitanala bahwa sistem di RS belum menerapkan *log-out* otomatis berdasarkan waktu, namun akun akan keluar otomatis saat komputer dimatikan atau aplikasi ditutup. Setiap pengguna memiliki akun pribadi berupa *username* dan *password* yang tidak digunakan bersama. Petugas rekam medis memiliki hak akses lebih luas karena bertugas mengelola data lintas unit, seperti ITD, poliklinik, rawat inap, dan laboratorium sesuai kewenangannya.

Informan 1: "Ya sejauh ini menurut saya Rekam Medis Elektronik di RSUP Dr. Sitanala sudah berjalan dengan baik. Untuk proses log – out di SIMRS, kalau komputer dimatikan atau aplikasinya

ditutup, maka sistem akan otomatis ter log – out. Jadi, saat komputer di-close, akun pengguna juga langsung log – out secara otomatis."

Informan 2: "Penggunaan username dan password di sistem sudah cukup aman karena setiap dokter punya akun masing-masing yang dibuat dan diatur oleh tim IT RSUP Dr. Sitanala. Password bersifat pribadi, hanya diketahui oleh dokter yang bersangkutan, dan bisa diganti kalau diperlukan. Dengan cara ini, data tetap rahasia dan sistem tidak bisa diakses oleh orang yang tidak berwenang."

Berdasarkan hasil wawancara dengan kepala rekam medis, petugas IT, dokter, dan perawat, diketahui bahwa penerapan aspek *privacy* dalam sistem RME di RSUP Dr. Sitanala telah dilakukan melalui penggunaan akun individual berupa *username* dan *password* bagi setiap pengguna. Hak akses diberikan sesuai dengan peran dan tanggung jawab masing-masing unit kerja, sehingga tidak seluruh pengguna dapat mengakses seluruh data pasien. Namun demikian, masih ditemukan kelemahan pada penerapan fitur *automatic log out* yang memiliki durasi cukup lama, yaitu sekitar 2 jam ketika sistem tidak digunakan. Kondisi ini berpotensi menimbulkan risiko akses tidak sah apabila komputer ditinggalkan dalam keadaan masih *login.* Secara teori, menurut (Pradita et al., 2022) aspek *privacy* dalam RME harus mencakup penggunaan akun individual, enkripsi data, pembatasan hak akses berbasis jaringan, serta penerapan automatic *log out* untuk mencegah akses tidak sah. Temuan penelitian ini menunjukkan bahwa penerapan akun individual sudah sesuai teori, tetapi durasi *log out* yang terlalu lama belum memenuhi standar keamanan ideal (5–15 menit).

Penerapan aspek *integrity* di RSUP dr. Sitanala bahwa pasien diberikan edukasi dan diminta persetujuan saat pendaftaran terkait akses data oleh sistem atau pihak terkait, seperti Satu Sehat. Persetujuan dicatat melalui menu centang pada sistem RME; jika pasien setuju data dapat diakses, jika tidak maka akses tidak diberikan. Keakuratan data dijaga melalui identitas unik berupa nomor rekam medis/ID untuk setiap pasien. Petugas juga melakukan verifikasi identitas saat pendaftaran, dan sistem otomatis membuat nomor rekam medis baru bagi pasien yang belum terdaftar.

Informan 6: "Setiap pasien yang datang diberi penjelasan dan diminta persetujuannya di Tempat Pendaftaran Pasien (TPP) tentang apakah datanya boleh diakses oleh sistem atau pihak terkait, misalnya aplikasi Satu Sehat. Persetujuan ini dicatat di sistem melalui menu centang saat pendaftaran. Kalau pasien setuju, data bisa diakses sesuai izin. Kalau tidak setuju, data tidak bisa diakses. Cara ini memastikan data pasien hanya dipakai dengan persetujuan mereka."

Informan 7: "Keaslian dan keakuratan data pasien juga dijaga dengan menggunakan identitas unik. Setiap pasien punya satu nomor rekam medis (ID) yang tidak bisa dipakai lebih dari satu orang. Saat pendaftaran, petugas mengecek identitas pasien seperti nama, tanggal lahir, alamat, dan nama ibu, untuk memastikan pasien sudah terdaftar atau belum. Kalau belum, sistem akan

membuatkan nomor rekam medis baru. Dengan begitu, identitas pasien terjamin asli dan data medisnya akurat."

Hasil wawancara menunjukkan bahwa integritas data pasien dijaga melalui pembatasan kewenangan dalam melakukan perubahan atau penghapusan data pada sistem RME. Tidak semua pengguna memiliki hak untuk mengedit data, dan perubahan data hanya dapat dilakukan oleh petugas yang berwenang sesuai dengan prosedur yang berlaku. Temuan ini menunjukkan bahwa aspek integrity di RSUP Dr. Sitanala telah sesuai dengan teori karena terdapat pembatasan hak edit dan hapus data. Hal ini juga selaras dengan penelitian yang menyatakan bahwa pembatasan kewenangan edit/hapus merupakan bentuk perlindungan integritas data. Dengan demikian, aspek *integrity* telah berjalan dengan baik widiyanti (Widiyanti et al., 2024).

Penerapan *authentication* di RSUP dr. Sitanala menggunakan mekanisme tanda tangan elektronik. Di unit rekam medis digunakan RM *signature* melalui pemindaian *barcode* nomor rekam medis; jika barcode terbaca, sistem otomatis memproses penandatanganan, sedangkan jika gagal akan kembali ke halaman awal. Apabila dokter mengalami kendala pada tanda tangan elektronik, PIN, sidik jari, atau file *signature*, masalah dilaporkan kepada tim IDP untuk ditindaklanjuti dengan metode alternatif seperti *barcode*. Sementara itu, perawat menyampaikan bahwa penggunaan tanda tangan elektronik berjalan baik dan belum ditemukan kendala signifikan.

Informan 1: "Di unit Rekam Medis, sistem menggunakan semacam tanda tangan elektronik yang disebut RM signature. Untuk menandatangani dokumen, petugas memindai barcode yang berisi nomor rekam medis pasien, bukan nama pasien. Kalau barcode terbaca dengan benar, sistem otomatis mengenali nomor rekam medis dan melanjutkan proses penandatanganan. Kalau barcode tidak terbaca, sistem akan kembali ke halaman awal supaya proses bisa diulang."

Informan 3: "Kalau ada masalah atau kendala saat menggunakan tanda tangan elektronik, PIN sidik jari, atau file signature, dokter langsung melaporkannya ke tim IDP. Tim IDP kemudian menindaklanjuti sesuai prosedur, misalnya dengan menggunakan barcode atau metode lain yang sudah ditetapkan. Dengan cara ini, proses pelayanan dan pencatatan tetap bisa berjalan meski ada kendala teknis."

Informan 4: "Menurut perawat, penggunaan tanda tangan elektronik sejauh ini berjalan lancar dan tidak ada kendala berarti. Meski proses verifikasi bukan tugas utamanya, penerapan tanda tangan elektronik di bagian perawat dinilai baik dan belum pernah ada masalah teknis yang dilaporkan.

Berdasarkan hasil wawancara, mekanisme *authentication* pada sistem RME di RSUP Dr. Sitanala dilakukan melalui proses *login* menggunakan *username* dan *password* yang bersifat individual. Setiap aktivitas pengguna terekam dalam sistem sehingga dapat diketahui identitas pengguna yang mengakses data. Autentikasi berbasis password saja memiliki potensi risiko seperti

brute force attack, phishing, dan *shoulder surfing*. Oleh karena itu, penerapan *multi-factor authentication* (MFA) atau OTP dinilai lebih aman (Zega et al., 2025).

Penerapan aspek *availability* di RSUP dr. Sitanala menjaga keamanan data pasien saat terhubung dengan pihak eksternal seperti BPJS Kesehatan melalui penggunaan API sebagai penghubung antara SIMRS dan sistem BPJS. Akses API dilindungi dengan *username*, *password*, serta token yang berlaku sekitar satu jam dan harus diperbarui secara berkala. Selain itu, rumah sakit menerapkan *backup* data otomatis setiap hari sekitar pukul 01.00 dini hari secara real time. Jika terjadi gangguan atau kehilangan data, proses pemulihan dapat dilakukan menggunakan data cadangan dan umumnya memerlukan waktu 1–2 jam.

Informan 8: "keamanan data pasien tetap terjaga meskipun sistem harus terhubung dengan pihak luar seperti BPJS Kesehatan. Pertukaran data dilakukan lewat web service atau API yang diberikan langsung oleh BPJS, dan hanya dipakai untuk mengirim data yang dibutuhkan. Akses ini dijaga ketat dengan username, password, dan token khusus yang cuma diketahui dan disimpan oleh petugas rumah sakit. Informasi ini tidak dibagikan ke pihak luar, jadi hanya petugas yang berwenang saja yang bisa mengelola pertukaran data antara rumah sakit dan BPJS."

Informan 6: "data pasien di-backup setiap hari secara otomatis pada waktu yang ditentukan sistem. Jadi, kalau terjadi gangguan, kehilangan data, atau serangan siber, data bisa dipulihkan dari backup terakhir, sehingga informasi pasien tetap aman dan tersimpan dengan baik."

Hasil wawancara menunjukkan bahwa ketersediaan data pada sistem RME di RSUP Dr. Sitanala didukung oleh sistem yang dapat diakses selama jam pelayanan serta adanya proses pencadangan data *(backup).* Meskipun demikian, rumah sakit pernah mengalami gangguan sistem akibat serangan siber yang menyebabkan *downtime* pada sistem pendaftaran *online* sementara. Hal ini selaras temuan bahwa aspek *availability* harus menjamin sistem dapat diakses kapan saja serta memiliki mekanisme pencadangan data untuk mencegah kehilangan informasi (Pradita et al., 2022). Penelitian lain juga menekankan bahwa keamanan informasi harus mampu mencegah gangguan operasional akibat serangan siber (Rachmadani et al., 2025).

Penerapan *acces control* di RSUP dr Sitanala bahwa petugas IT mengatur hak akses pengguna dengan memberikan *username* dan *password* masing-masing serta membatasi akses modul sesuai unit kerja dan tugas, seperti poliklinik, rawat inap, pendaftaran, atau kasir. Dengan demikian, pengguna hanya dapat mengakses sistem sesuai kewenangannya. Akses data pasien juga harus melalui persetujuan pasien saat pendaftaran. Jika pasien menyetujui, petugas menandai persetujuan di SIMRS sehingga data dapat diakses oleh sistem terkait seperti Satu Sehat. Jika tidak disetujui, data tidak dapat diakses. Mekanisme ini menjadi bentuk legalitas sekaligus perlindungan privasi pasien.

Informan 6: "Setiap pengguna punya username dan password sendiri, dan aksesnya diatur sesuai dengan unit kerja dan tugasnya. Misalnya, kalau seorang petugas hanya boleh masuk ke

modul poliklinik, dia tidak bisa mengakses modul rawat inap, begitu juga sebaliknya. Aturan yang sama berlaku untuk unit lain seperti pendaftaran atau kasir. Dengan cara ini, hanya orang yang berwenang saja yang bisa mengakses bagian sistem sesuai tugasnya."

Informan 7: "Akses ke data pasien hanya diberikan kalau ada izin yang sah dan bisa dipertanggungjawabkan. Permintaan akses harus dari pegawai RSUP Dr. Sitanala yang jelas identitas dan tugasnya. Kalau permintaan datang dari orang luar atau yang tidak bekerja di rumah sakit, tidak akan diproses. Proses akses baru bisa dilakukan kalau ada permohonan resmi, misalnya dari perawat atau unit terkait untuk buat akun dokter baru. Permohonan ini harus pakai formulir tertulis yang diisi lengkap, ditandatangani, dan mencantumkan data penting seperti nama lengkap, modul atau layanan yang dibutuhkan, serta nickname khusus sebagai identitas unik untuk validasi. Dengan cara ini, akses ke data pasien tetap terkontrol dan aman."

Berdasarkan hasil wawancara, kontrol akses pada sistem RME diterapkan melalui pembatasan hak akses berdasarkan jabatan dan unit kerja. Kepala rekam medis dan unit IT memiliki kewenangan lebih luas dibandingkan dengan dokter atau perawat dalam mengakses dan mengelola data tertentu. Menurut (Pradita et al., 2022), *access control* dilakukan melalui pembatasan *user ID* dan *password* serta pengaturan hak akses berbasis peran *(role-based access control).* Selain itu, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi menegaskan bahwa pengolahan data harus dilakukan sesuai prinsip pembatasan tujuan dan otorisasi yang sah.

Penerapan aspek non-repudiation di RSUP Dr. Sitanala dilakukan melalui pencatatan seluruh aktivitas pengguna dalam database, seperti tanggal pembuatan dan pembaruan data serta identitas pengguna yang melakukan tindakan tersebut. Dengan mekanisme ini, setiap perubahan data pasien dapat ditelusuri secara jelas. Selain itu, setiap pengguna memiliki username dan password pribadi, dengan password disimpan dalam bentuk terenkripsi (hash) sehingga tidak dapat diketahui pihak lain, termasuk administrator. Sistem ini menjaga akuntabilitas, keamanan akses, dan keaslian data pasien.

Informan 6: "Setiap kegiatan di sistem dicatat dalam tabel di database. Di tiap tabel ada kolom khusus yang menyimpan informasi penting, seperti kapan data dibuat (create date), siapa yang membuatnya (user create), kapan data diperbarui (update date), dan siapa yang memperbarui (user update). Dengan begitu, setiap tindakan bisa dilacak dengan jelas, misalnya siapa yang mendaftarkan pasien atau siapa yang mengubah data pasien tertentu. Sistem log file ini membuat semua aktivitas tercatat detail dan bisa diperiksa, sehingga data pasien tetap terjaga keasliannya dan bisa dipertanggungjawabkan."

Informan 7: "Akses ke sistem dibatasi supaya tidak bisa digunakan sembarangan oleh orang yang tidak berhak. Caranya mirip seperti kunci pribadi yang cuma bisa dipakai oleh pemiliknya, sedangkan kunci publik terkait dengan akses ke sistem atau aplikasi tertentu sesuai hak yang diberikan. Untuk akun eksternal atau yang dibuat pasien, pengelolaan password menjadi tanggung

jawab masing-masing pengguna, dan tersedia fitur "lupa password" kalau dibutuhkan. Selain itu, pihak rumah sakit juga mencatat akses secara terbatas sebagai langkah keamanan tambahan dan untuk bisa ditelusuri kalau perlu audit, sehingga data tetap aman dan rahasia."

Hasil wawancara menunjukkan bahwa sistem RME di RSUP Dr. Sitanala telah memiliki fitur pencatatan aktivitas *(log activity)* yang merekam setiap tindakan pengguna, seperti pengisian, perubahan, dan penghapusan data. Fitur ini memungkinkan penelusuran kembali apabila terjadi kesalahan atau sengketa data. Menurut (Tiorentap, 2020). aspek *non-repudiation* bertujuan mencegah pengguna menyangkal aktivitas yang telah dilakukan melalui pencatatan log dan sistem jejak audit (audit trail). temuan lain juga menekankan pentingnya pencatatan aktivitas pengguna sebagai bentuk pertanggungjawaban (Pradita et al., 2022).

Kesimpulan

Berdasarkan hasil penelitian dan pembahasan mengenai tinjauan aspek keamanan informasi data pasien dalam penerapan Rekam Medis Elektronik (RME) di RSUP Dr. Sitanala, maka dapat ditarik beberapa kesimpulan sebagai berikut:

Penerapan aspek privasi pada sistem RME di RSUP Dr. Sitanala telah dilakukan melalui penggunaan *username* dan *password* untuk setiap pengguna serta pembatasan akses sesuai kewenangan. Namun demikian, penerapan *automatic log out* masih belum optimal karena waktu *log out* otomatis relatif lama, sehingga berpotensi menimbulkan risiko akses tidak sah apabila sistem ditinggalkan dalam keadaan aktif.

Aspek integritas data pasien telah diterapkan dengan baik, ditunjukkan melalui pembatasan kewenangan dalam pengubahan dan penghapusan data. Perubahan data hanya dapat dilakukan oleh petugas yang memiliki hak akses tertentu, sehingga keakuratan dan keutuhan data rekam medis tetap terjaga.

Proses autentikasi pada sistem RME telah diterapkan melalui mekanisme *login* menggunakan identitas pengguna. Sistem ini mampu memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses data pasien, meskipun masih terdapat peluang peningkatan keamanan melalui penguatan metode autentikasi berlapis.

Ketersediaan data pada sistem RME di RSUP Dr. Sitanala secara umum telah terjaga, di mana data dapat diakses oleh petugas berwenang sesuai kebutuhan pelayanan. Selain itu, telah dilakukan upaya pencadangan data untuk mencegah kehilangan informasi, meskipun kejadian gangguan sistem akibat serangan siber menunjukkan perlunya penguatan sistem cadangan dan pemulihan data.

Penerapan kontrol akses telah dilakukan dengan pembagian hak akses berdasarkan peran dan tanggung jawab masing-masing pengguna. Hal ini membantu mencegah penyalahgunaan data serta membatasi akses hanya pada informasi yang relevan dengan tugas pengguna.

Pada sistem RME telah diterapkan melalui pencatatan aktivitas pengguna dalam bentuk log sistem. Dengan adanya log aktivitas, setiap tindakan yang dilakukan pengguna dapat ditelusuri sehingga meminimalkan kemungkinan penyangkalan terhadap aktivitas yang telah dilakukan dalam sistem.

Ucapan Terimakasih

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Universitas Esa Unggul atas dukungan, ilmu, serta fasilitas yang diberikan selama proses perkuliahan dan penyusunan penelitian ini. Terima kasih juga disampaikan kepada para dosen, pembimbing, staf akademik, serta seluruh pihak yang telah memberikan arahan, motivasi, dan bantuan sehingga penelitian ini dapat diselesaikan dengan baik.

Referensi

Ardianto, E. T., Sabran, & Nurjanah, L. (2024). Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik Di Rumah Sakit X. *Jurnal Rekam Medik & Manajemen Informasi Kesehatan*, *3*(2), 18–30. https://doi.org/https://doi.org/10.47134/rmik.v3i2.54

Christianto, H., & Dewi, E. D. A. M. (2022). Tindakan Membuka Identitas Pasien Terkonfirmasi Covid-19 oleh Rumah Sakit Berdasarkan Hak Asasi Manusia dan Hukum Pidana. *Jurnal HAM*, *13*(1), 131–150. https://doi.org/10.30641/ham.2022.13.131-150

Himastuti, R., Pinandito, A., & Pradana, F. (2023). Analisis Penerimaan Rekam Medis Elektronik (RME) di Puskesmas dengan menggunakan Technology Acceptance Model (TAM). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *7*(5), 2628–2633. http://j-ptiik.ub.ac.id

Kemenkes RI. (2020). *Peraturan Menteri Kesehatan Republik Indonesia Nomor 3 Tahun 2020 Tentang Klasifikasi Dan Perizinan Rumah Sakit*.

Melisa, N. P., Sukmaningsih, W. R., & Licia, R. (2024). *Analisis Rekam Medis Elektronik Rawat Jalan Pada Aspek Keamanan Data Pasien Di Rumah Sakit Umum Daerah Dr . Soediran Mangun Sumarso Wonogiri*. *03*(03), 160–168.

Permenkes No. 24. (2022). *Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 Tentang Rekam Medis*. https://peraturan.bpk.go.id/Details/245544/permenkes-no-24-tahun-2022

Pradita, R., Kusumo, R., & Rahmawati. (2022). Pentingnya Aspek Keamanan Informasi Data Pasien Pada Penerapan Rme Di Puskesmas. *Journal Of Sustainable Community Service*, *2*(2), 52–62. Https://Doi.Org/10.55047/Jscs.V2i2.437

Rachmadani, A., Yulianti, N. T., Sasanti, D. A., Sari, H. E., & Wulandari, P. (2025). Analisis Penggunaan Rekam Medis Elektronik Dengan Kepuasaan Tenaga Kesehatan Di Puskemas Karang Joang Kota Balikpapan. *Jurnal Kajian Ilmiah Kesehatan Dan Teknologi*, *7*(1), 149–156. https://doi.org/10.52674/jkikt.v7i1.238

Tiorentap, D. R. A. (2020). Evaluasi Manfaat Penerapan Rekam Medis Elektronik di Negara Berkembang: Systematic Literature Review. *INOHIM*, *8*(2i), 69–79. https://doi.org/https://doi.org/10.47007/inohim.v8i2.218

Widiyanti, S. W., Hastuti, N. M., & Kusumawati, E. A. (2024). Tinjauan Keamanan Data Rekam Medis Elektronik Pada Aplikasi Simpus Berdasarkan Aspek Confidentiality, Integrity, Dan Availability Di Puskesmas Tasikmadu Karanganyar. *Indonesian Journal of Health Information Management*, *4*(2), 1. https://doi.org/10.54877/ijhim.v4i2.212

Zega, E. B., Ginting, W., & Damanik, R. (2025). Sistem Keamanan Login Menggunakan Metode Autentikasi Dua Faktor Dengan Verifikasi Gambar. *International Multidiciplinary Journal*, *1*(2), 25–35. https://sorakgemaintelektual.com/jurnal/index.php/imun/article/view/127