

BAB I

PENDAHULUAN

A. Latar Belakang

Rumah sakit adalah fasilitas pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan perseorangan secara paripurna melalui pelayanan kesehatan promotif, preventif, kuratif, rehabilitatif, dan paliatif dengan menyediakan pelayanan rawat inap, rawat jalan, dan gawat darurat (Undang-Undang Kesehatan Nomor 17, 2023). Pelaksanaan fungsi tersebut menuntut rumah sakit untuk memiliki sistem pengelolaan informasi yang efektif dan efisien guna mendukung mutu pelayanan kesehatan, salah satunya melalui penyelenggaraan sistem rekam medis. Rekam medis merupakan dokumen yang berisi data identitas pasien, hasil pemeriksaan, pengobatan, tindakan, serta pelayanan lain yang telah diberikan kepada pasien (Permenkes RI Nomor 24, 2022).

Seiring dengan perkembangan teknologi informasi, sistem pencatatan rekam medis mengalami transformasi dari bentuk manual ke bentuk elektronik. Pemerintah Indonesia secara resmi mewajibkan penerapan Rekam Medis Elektronik (RME) pada seluruh fasilitas pelayanan kesehatan sebagaimana diatur dalam Peraturan Menteri Kesehatan RI Nomor 24 Tahun 2022 tentang Rekam Medis. Rekam Medis Elektronik (RME) adalah rekam medis yang dibuat menggunakan sistem elektronik yang diperuntukkan bagi penyelenggaraan rekam medis (Permenkes RI Nomor 24, 2022).

Penerapan Rekam Medis Elektronik memiliki berbagai keunggulan, antara lain efisiensi waktu, kemudahan akses data, dan pengurangan risiko kehilangan dokumen fisik. Pemerintah Indonesia mendukung penuh transisi ini dengan mewajibkan seluruh Fasilitas Pelayanan Kesehatan (Fasyankes) di Indonesia untuk menyelenggarakan RME paling lambat 31 Desember 2023 (Permenkes RI Nomor 24, 2022). Namun demikian, penerapan Rekam Medis Elektronik menimbulkan tantangan baru, khususnya terkait keamanan data rekam medis.

Keamanan data rekam medis merupakan upaya perlindungan fisik dan elektronik untuk menjamin kerahasiaan, keutuhan, dan ketersediaan informasi kesehatan serta melindungi privasi pasien (Ekasari, 2025). Data rekam medis memiliki sifat sensitif dan rahasia sehingga memerlukan sistem pengamanan yang kuat agar tidak disalahgunakan oleh pihak yang tidak berwenang. Kondisi keamanan data kesehatan di Indonesia masih menghadapi berbagai tantangan yang signifikan.

Pada tahun 2022 terjadi kebocoran data rekam medis milik sekitar 6 juta pasien COVID-19 yang berasal dari sistem Kementerian Kesehatan RI. Data bocor diunggah pada Kamis, 6 Januari 2022 berukuran sekitar 720 GB tersebut berisi informasi medis dan identitas pasien, seperti hasil pemeriksaan, hasil tes COVID-19, data radiologi, dan data diagnostik seperti, keluhan sesak nafas, saturasi rendah, dari berbagai rumah sakit di Indonesia. Kebocoran data ini menunjukkan masih lemahnya sistem keamanan data kesehatan digital serta

berpotensi menimbulkan pelanggaran privasi dan penyalahgunaan data pasien (Nadiroh and Wiraguna, 2025).

Fenomena tersebut menunjukkan bahwa risiko kebocoran data RME masih menjadi permasalahan serius di fasilitas pelayanan kesehatan. Penelitian sebelumnya menunjukkan kebocoran data RME tetap terjadi meskipun sistem keamanan telah diterapkan. Penelitian di RS P Surakarta mengungkapkan bahwa risiko kebocoran disebabkan oleh kondisi fisik, human error, kegagalan sistem komputer, interaksi pengguna dengan sistem, kompleksitas infrastruktur teknologi informasi, serta ancaman peretasan dari pihak luar (Budiman, Isa and Soekiswati, 2025). Selain itu, kebocoran data pada aplikasi PeduliLindungi yang kemudian bertransformasi menjadi SATUSEHAT juga menimbulkan kekhawatiran akan risiko kebocoran data kesehatan secara berkelanjutan (Yanto *et al.*, 2025).

Penelitian lain menunjukkan bahwa kebocoran data RME masih terjadi meskipun pembatasan hak akses dan SOP keamanan telah diterapkan. Hal ini disebabkan oleh *password* yang tidak diganti secara berkala, SOP keamanan yang belum memadai, serta kontrol akses yang belum efektif. Selain itu, praktik berbagi kata sandi antarpetugas juga meningkatkan risiko pelanggaran privasi pasien (Sofia *et al.*, 2022) .

Meskipun sistem telah dilengkapi dengan *server* cadangan, antivirus, dan tanda tangan elektronik, faktor manusia tetap menjadi celah utama dalam sistem keamanan informasi (Nugroho and Kurniadi, 2022). Selain itu, aspek autentikasi juga masih menjadi tantangan, di mana sebanyak 60% petugas

menggunakan kombinasi *username* dan *password* yang lemah, serta 15% akun administrator memiliki hak akses yang terlalu luas sehingga meningkatkan potensi terjadinya ancaman dari dalam sistem (Setyaningrum and Ricky, 2025). Kondisi tersebut menunjukkan bahwa penerapan aspek keamanan data rekam medis elektronik berdasarkan prinsip CIA Triad, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*), belum sepenuhnya optimal.

Prinsip kerahasiaan (*confidentiality*) menjamin bahwa informasi pasien hanya dapat diakses oleh pihak yang berwenang (Rani *et al.*, 2025). Prinsip integritas (*integrity*) menjamin bahwa data tetap akurat, utuh, dan tidak mengalami perubahan tanpa izin pihak berwenang (Rohman *et al.*, 2025). Sementara itu, prinsip ketersediaan (*availability*) memastikan bahwa data dapat diakses oleh pengguna yang berhak kapan pun diperlukan untuk mendukung pelayanan kesehatan (Ardianto and Nurjanah, 2024).

Berdasarkan studi pendahuluan yang dilakukan pada 23 November 2025, RSPAU dr. S. Hardjolukito merupakan Rumah Sakit Pusat Angkatan Udara yang melayani personel militer maupun masyarakat umum. Penerapan sistem Rekam Medis Elektronik (RME) dengan aplikasi SIMETRIS (Sistem Informasi Manajemen Terintegrasi Rumah Sakit) di RSPAU dr. S. Hardjolukito bermula pada tahun 2022 yang dikembangkan oleh IT internal rumah sakit dengan melalui kerja sama dengan tim *development* RSUP Dr. Sardjito.

Pada sistem SIMETRIS di rumah sakit fitur *automatic logout* belum diterapkan, sehingga berpotensi meningkatkan risiko akses tidak sah apabila pengguna lupa keluar dari sesi aktif. Meskipun mendukung akses pada dua perangkat komputer dengan ketentuan *logout* pada satu komputer memutuskan sesi di semua perangkat. Penggunaan *username* dan *password* individual telah diterapkan bagi setiap pegawai, namun masih terdapat kelemahan berupa penyimpanan kata sandi secara otomatis dalam sistem yang berpotensi disalahgunakan oleh pegawai lain. Kondisi tersebut menunjukkan perlunya penguatan kontrol akses pada SIMETRIS untuk menjaga privasi data pasien. Selain itu, ketersediaan fitur tanda tangan digital bagi dokter untuk memvalidasi akses dan entri data melalui mekanisme autentikasi berlapis, sehingga berperan penting dalam mencegah akses tidak sah pada sistem SIMETRIS.

Perubahan data rekam medis pada sistem SIMETRIS dapat dilakukan maksimal dalam waktu 2x24 jam oleh pengguna berwenang. Setelah melewati batas tersebut, diperlukan nota dinas perubahan data secara resmi. Sistem *backup* data beroperasi otomatis setiap hari pada *server* internal rumah sakit di Ruang INFOLAHTA (Informasi dan Pengolahan Data) mendukung untuk keamanan data informasi. Mekanisme ini mengantisipasi *downtime* dengan menyediakan cadangan data pasien.

Berdasarkan latar belakang yang telah diuraikan, penelitian ini dilakukan untuk menganalisis persepsi petugas RM terhadap keamanan data Rekam Medis Elektronik berdasarkan aspek CIA Triad (*confidentiality*, *integrity*, dan

availability). Maka dari itu, peneliti tertarik melakukan penelitian berjudul “Analisis Persepsi Petugas RM Terhadap Keamanan Data RME Berdasarkan Aspek *Confidentiality*, *Integrity*, Dan *Availability* (CIA) di RSPAU dr. S. Hardjolukito Tahun 2026”.

B. Rumusan Masalah

Penerapan Rekam Medis Elektronik (RME) berpotensi menimbulkan risiko terhadap keamanan data apabila tidak dikelola sesuai standar yang berlaku. Oleh karena itu, rumusan masalah dalam penelitian ini adalah:

“Bagaimana Analisis Persepsi Petugas RM Terhadap Keamanan Data RME Berdasarkan Aspek *Confidentiality*, *Integrity*, Dan *Availability* (CIA) di RSPAU dr. S. Hardjolukito Tahun 2026?”

C. Tujuan Penelitian

1. Tujuan Umum

Menganalisis persepsi petugas RM terhadap keamanan data RME berdasarkan aspek *Confidentiality*, *Integrity*, dan *Availability* (CIA) di RSPAU dr. S. Hardjolukito tahun 2026.

2. Tujuan Khusus

- a. Menganalisis persepsi petugas RM terhadap keamanan data Rekam Medis Elektronik berdasarkan aspek *confidentiality*.
- b. Menganalisis persepsi petugas RM terhadap keamanan data Rekam Medis Elektronik berdasarkan aspek *integrity*.

- c. Menganalisis persepsi petugas RM terhadap keamanan data Rekam Medis Elektronik berdasarkan aspek *availability*.

D. Ruang Lingkup

1. Ruang Lingkup Waktu

Penelitian ini dilaksanakan pada tanggal 15 – 27 April 2026.

2. Ruang Lingkup Tempat

Penelitian ini dilaksanakan di RSPAU dr. S. Hardjolutomo yang beralamat di Jl. Majapahit, Karang Janbe, Kec. Banguntapan, Kab. Bantul, Daerah Istimewa Yogyakarta 55198.

3. Ruang Lingkup Materi

Materi penelitian ini mengenai keamanan data rekam medis elektronik.

4. Ruang Lingkup Metode

Metode yang digunakan dalam penelitian ini yaitu dengan metode kuantitatif pendekatan deskriptif dengan kuesioner.

E. Manfaat Penelitian

Penelitian ini diharapkan akan memberikan manfaat bagi beberapa pihak sebagai berikut:

1. Manfaat Teoritis

Penelitian ini secara teoritis memperdalam pemahaman implementasi CIA (*Confidentiality, Integrity, dan Availability*) RME di rumah sakit dengan praktik lapangan untuk analisis risiko, serta mendukung pengembangan model keamanan efektif.

2. Manfaat Praktis:

a. Bagi Rumah Sakit RSPA dr. S. Hardjolukito:

Penelitian ini diharapkan dapat menjadi bahan evaluasi bagi RSPA dr. S. Hardjolukito dalam meningkatkan pengendalian akses, penggunaan akun, serta pengelolaan *backup* dan monitoring sistem SIMETRIS. Selain itu, petugas rekam medis diharapkan mematuhi kebijakan keamanan data melalui penggunaan akun secara individual dan akses data sesuai kewenangan guna mendukung perlindungan data pasien.

b. Bagi Poltekkes Kemenkes Yogyakarta:

Penelitian ini diharapkan dapat menjadi referensi pembelajaran untuk meningkatkan kompetensi dan pemahaman praktis dalam pengelolaan keamanan data Rekam Medis Elektronik serta penerapannya di dunia kerja.

c. Bagi Peneliti:

Penelitian ini diharapkan dapat meningkatkan kemampuan peneliti dalam menerapkan metode penelitian kuantitatif untuk menganalisis persepsi petugas RM terhadap keamanan Rekam Medis Elektronik berdasarkan aspek kerahasiaan, integritas, dan ketersediaan, serta menjadi bekal pengembangan kompetensi akademik di bidang keamanan informasi kesehatan.

F. Keaslian Penelitian

Penelitian mengenai “Analisis Persepsi Petugas RM Terhadap Keamanan Data RME Berdasarkan Aspek *Confidentiality*, *Integrity*, dan *Availability* di RSPAU dr. S. Hardjolukito Tahun 2026” belum pernah dilakukan sebelumnya. Adapun penelitian serupa dan pernah dilakukan, antara lain:

Tabel 1. Keaslian Penelitian

No.	Peneliti	Judul Penelitian	Metode	Hasil	Persamaan/Perbedaan
1.	Muhammad Rakha Pratama Nugroho, Arif Kurniadi (2022).	Tinjauan Tata Kelola Keamanan RME Berdasarkan Prinsip Keamanan PMK No. 24 Tahun 2022 di RSUD Dr. H Soewondo Kendal.	Metode pendekatan kualitatif deskriptif.	- Aspek Kerahasiaan, yaitu masih lemah pertukaran <i>password</i> meskipun ada pembatasan akses. - Aspek Integritas, yaitu terdapat fitur tanda tangan digital (<i>barcode</i>), perbaikan data maksimal 2x24 jam sesuai peraturan. - Aspek Ketersediaan, yaitu sebagian baik SOP Pelepasan informasi tapi ketidaksesuaian usia di bawah umur.	Persamaan: Penelitian ini sejalan dengan studi sebelumnya yang juga menyoroti aspek kerahasiaan, integritas, dan ketersediaan data RME. Perbedaan: Penelitian ini ditemukan pertukaran <i>password</i> di RSUD Dr. H. Soewondo Kendal yang belum tertangani pelatihan, serta ketidaksesuaian SOP usia minor.
2.	Siti Sofia, Efri Tri Ardianto, Ni-	Analisis Aspek Keamanan Informasi Pasien Pada Pe-	<i>Literature Review</i> (Tinjauan Pustaka).	Aspek Keamanan Informasi Data Pasien pada penerapan Rekam	Persamaan: Penelitian sebelumnya yang menunjukkan adanya kesenjangan

No.	Peneliti	Judul Penelitian	Metode	Hasil	Persamaan/Perbedaan
	yalatul Mu- na, Sabran (2022).	nerapan RME di Fasilitas Kesehatan (<i>Literature Review</i>).		Medik Elektronik (RME) yang terdiri dari 6 aspek utama: 1. <i>Confidentiality</i>: sudah menerapkan login dengan <i>username</i> dan <i>password</i>, <i>automatic log-off</i>, namun beberapa fasilitas belum optimal kerahasiaannya. 2. <i>Integrity</i>: perubahan atau penghapusan data hanya bisa dilakukan oleh administrator. 3. <i>Authentication</i>: sudah menerapkan tanda tangan digital. 4. <i>Availability</i>: penerapan Rekam Medis Elektronik di fasyankes sudah terintegrasi dengan sistem informasi khususnya BPJS kesehatan, serta menggunakan proses backup data guna mengantisipasi peretasan data pasien. 5. <i>Access Control</i>: dengan dilakukannya pembatasan hak akses dengan peng-	pada autentikasi dan kontrol akses keamanan. Perbedaan: Penelitian ini orisinal dengan fokus di Indonesia, cakupan data luas, menekankan aspek <i>non-repudiation</i> dan rekomendasi teknis khusus.

No.	Peneliti	Judul Penelitian	Metode	Hasil	Persamaan/Perbedaan
				gunaan <i>user id</i> dan <i>password</i> bagi masing-masing pengguna, serta kebijakan pengaksesan data harus seizin pemilik data. 6. <i>Non-Repudiation</i>: pada penerapan RME sudah diterapkan dengan adanya <i>log file</i> untuk melihat proses transaksi serta penggunaan kunci pulik dan pribadi.	
3.	Efri Tri Ardianto, Sabran, dan Lensa Nurjanah (2024).	Analisis Aspek Keamanan Data Pasien dalam Implementasi Rekam Medis Elektronik di Rumah Sakit X.	Dalam jurnal ini penelitian tersebut menggunakan metode kualitatif dengan menggunakan wawancara, observasi, dan dokumentasi.	1. Aspek Kerahasiaan (<i>Confidentiality</i>): login menggunakan <i>username</i> dan <i>password</i>, namun belum dilakukan secara berkala dan belum ada SOP khusus terkait keamanan data pasien. 2. Aspek Integritas (<i>Integrity</i>): fitur edit dan hapus data sudah ada, tetapi hanya bisa digunakan sesuai hak akses dan harus sesuai dengan SOP.	Persamaan: Penelitian ini mengkaji enam aspek keamanan informasi dan menemukan celah pada autentikasi dan kontrol akses. Perbedaan: Penelitian ini orisinal karena menggunakan studi kasus kualitatif mendalam, bukan hanya tinjauan pustaka, sehingga menghasilkan temuan empiris dan rekomendasi operasional.

No.	Peneliti	Judul Penelitian	Metode	Hasil	Persamaan/Perbedaan
				3. Aspek Autentikasi (<i>Authentication</i>): tanda tangan elektronik sudah diterapkan untuk dokter, namun untuk pasien masih manual.	
				4. Aspek Ketersediaan (<i>Availability</i>): rekam medis elektronik hanya bisa diakses di lingkungan rumah sakit dengan jaringan khusus guna memudahkan akses tetapi semua poli bisa mengakses data pasien.	
				5. Aspek Kontrol Akses (<i>Access Control</i>): pembatasan hak akses menggunakan <i>username</i> dan <i>password</i> , namun tampilan menu sama meskipun hak akses berbeda.	
				6. Aspek Nir-sangkal (<i>Non-repudiation</i>): sudah terdapat log data yang merekam riwayat akses dan pengeditan oleh pengguna, namun audit internal belum dilakukan secara rutin.	

No.	Peneliti	Judul Penelitian	Metode	Hasil	Persamaan/Perbedaan
4.	Untung Slamet Suhariyono, Fita Rusdian Ika-wati, dan Nur Afifah (2025).	Analisis Aspek Keamanan Informasi Data Pasien pada Rekam Medis Elektronik di UPT Puskesmas Karangploso.	Deskriptif kualitatif dengan wawancara dan observasi pada 4 informan (kepala rekam medis, petugas IT, pendaf-taran, dan perawat).	Keamanan data pada aplikasi E-Puskesmas sudah baik: 1. <i>Confidentiality</i> dijaga dengan <i>username</i>, <i>password</i>, dan <i>log out</i> otomatis. 2. <i>Integrity</i> aman karena hanya petugas berwenang yang dapat mengubah data. 3. <i>Availability</i> terjamin karena data tersimpan otomatis 25 tahun dan didukung genset serta internet stabil.	Persamaan: Penelitian ini menekankan perlindungan data lewat akses terbatas dan <i>logout</i> otomatis. Perbedaan: Penelitian ini berbeda karena dilakukan di Puskesmas dengan aplikasi E-Puskesmas yang terintegrasi ke Dinas Kesehatan, bukan di rumah sakit.