BAB 1. PENDAHULUAN

1.1 Latar Belakang

Berkembangnya teknologi informasi dalam berbagai aspek kehidupan termasuk bidang kesehatan telah membawa dampak yang signifikan. Di tengah era digitalisasi ini, penyedia layanan kesehatan mendapatkan manfaat besar, salah satunya adalah tersedianya informasi pasien secara tepat waktu. Teknologi ini memungkinkan koordinasi perawatan yang lebih optimal serta peningkatan kualitas layanan kesehatan di institusi seperti rumah sakit (Mahdani et al., 2023).

Sebagai institusi pelayanan, rumah sakit memiliki peran penting dalam menyediakan layanan promotif, preventif, kuratif, dan rehabilitatif. Cakupan layanan tersebut meliputi rawat inap, rawat jalan, serta gawat darurat (Presiden Republik Indonesia, 2023). Untuk menjamin pelayanan kesehatan dapat berjalan dengan baik, diperlukan infrastruktur sistem yang baik pula, salah satunya melalui pengelolaan rekam medis yang efektif.

Rekam medis elektronik muncul sebagai inovasi penting dalam manajemen data medis di fasilitas kesehatan. Sistem ini memfasilitasi akses terhadap informasi pasien secara lebih efektif dan efisien, sehingga dapat mendukung pengambilan keputusan klinis yang tepat. Selain itu, integrasi data antar sistem manajemen rumah sakit dengan sistem lainnya juga menjadi lebih mudah, dan memungkinkan kolaborasi yang lebih baik di antara tenaga medis (Mahdani et al., 2023). Meskipun demikian, penerapan rekam medis elektronik menghadapi sejumlah tantangan dan risiko, terutama terkait dengan keamanan sistem informasi. Oleh karena itu, rumah sakit perlu merancang strategi yang komprehensif untuk mengantisipasi potensi ancaman dan permasalahan yang mungkin muncul selama proses implementasi, agar sistem ini dapat berfungsi secara optimal dan aman (Asih et al., 2024).

Keamanan sistem informasi merupakan aspek yang sangat penting di era digital saat ini terutama untuk melindungi data dari akses, penyalahgunaan,

atau manipulasi oleh pengguna yang tidak berwenang untuk memastikan kerahasiaan, integritas, dan kemudahan penggunaan (Nurul et al., 2022). Pemilik sistem informasi perlu mengambil langkah-langkah strategis untuk memastikan perlindungan data, seperti menerapkan pembatasan akses bagi pihak yang berwenang dan memastikan mekanisme penyimpanan data yang aman (Asih et al., 2024). Tantangan dalam menjaga keamanan informasi ini semakin meningkat seiring dengan pertumbuhan pengguna internet yang diikuti oleh lonjakan kejahatan siber terutama pada data kesehatan, khususnya yang berasal dari rekam medis elektronik (Herisasono, 2024).

Rumah Sakit Tingkat III Baladhika Husada Jember merupakan institusi yang telah menerapkan rekam medis elektronik sejak 2018 perlu menjaga keamanan sistem yang ada. Dari hasil studi pendahuluan yang dilakukan peneliti ke petugas IT ditemukan beberapa permasalahan yang bisa mempengaruhi keamanan sistem informasi dalam penerapan rekam medis elektronik di Rumah Sakit Tingkat III Baladhika Husada Jember. Salah satu temuan berkaitan dengan belum diterapkannya kebijakan manajemen kata sandi. Hal tersebut dibuktikan melalui pernyataan petugas IT yang menjelaskan bahwa:

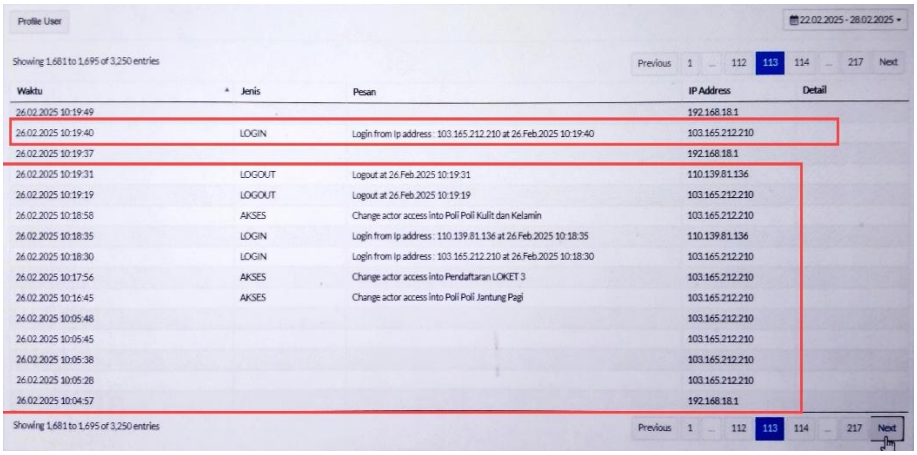
> "*Sejauh ini belum ada pembatasan atau aturan terkait sandi harus kompleks dengan huruf, angka, simbol serta belum terdapat ketentuan mengenai jumlah minimal karakter"*
>
> (Informan 3, 2025)

Hasil wawancara tersebut menunjukkan bahwa sistem saat ini belum mengatur jumlah karakter, dan kombinasi jenis karakter. Hal ini berhubungan dengan aspek kerahasiaan dalam hal autentikasi karena kata sandi yang tidak kompleks dapat membuat sistem lebih rentan terhadap serangan *brute force* atau percobaan peretasan lainnya (Sofia et al., 2022). Hal tersebut sejalan dengan penelitian Ritonga et al. (2025) yang mengacu pada rekomendasi *National Institute of Standards and Technology* (NIST), yang menyarankan penggunaan kata sandi sepanjang 12-16 karakter dengan variasi jenis karakter untuk meningkatkan kompleksitas dan memperluas kemungkinan kombinasi,

sehingga mampu memberikan tingkat perlindungan yang lebih baik terhadap berbagai ancaman keamanan.

Berdasarkan hasil observasi, diketahui bahwa seluruh perawat di instalasi rawat jalan menggunakan satu akun yang sama, yaitu akun milik petugas administrasi instalasi rawat jalan. Hal ini tidak sesuai dengan prinsip Kerahasiaan (*Confidentiality*), tepatnya terkait kontrol akses, karena setiap pengguna seharusnya memiliki akun masing-masing sesuai tugas dan kewenangan yang ada (Sofia et al., 2022).

Selain itu, untuk memastikan apakah seluruh aktivitas pengguna tercatat dengan baik pada sistem, peneliti meninjau menu *audit log* yang tersedia pada rekam medis elektronik. Berikut salah satu tampilan *audit log* yang ada pada RME sebagai berikut:

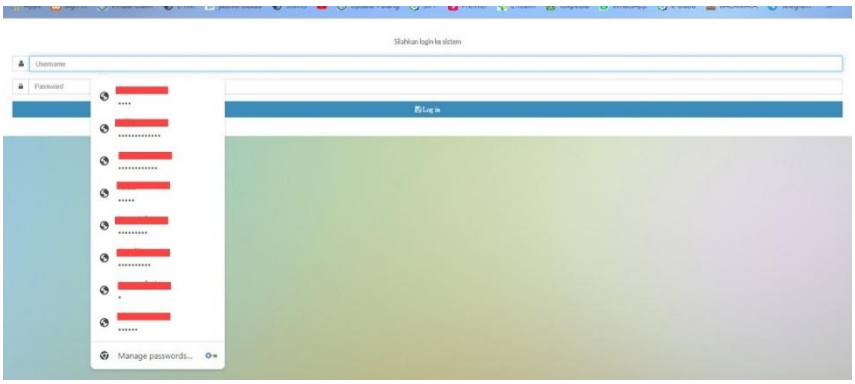


Gambar 1.1 *Audit Log* Rekam Medis Elektronik

Berdasarkan gambar 1.1 ditemukan bahwa sistem rekam medis elektronik berbasis web ini terdapat satu akun pengguna digunakan oleh beberapa orang petugas secara bergantian dan tidak disertai fitur *automatic logout* apabila terdapat penggunaan akun secara bersamaan yang terlihat dari adanya beberapa sesi masuk baru tanpa adanya proses *logout* dari sesi sebelumnya. Hal ini menunjukkan adanya kelemahan pada aspek kerahasiaan, khususnya dalam proses autentikasi identitas pengguna, karena sistem tidak mampu memastikan siapa pemilik akses yang sebenarnya maupun aktivitas apa saja yang dilakukan oleh masing-masing pengguna (Wardani et al., 2024).

Selain itu, pada *audit log* ada beberapa aktivitas yang dilakukan pengguna tidak terekam pada menu tersebut. Kondisi ini menunjukkan lemahnya integritas data, khususnya dalam pencatatan log. Masalah ini menyebabkan lemahnya sistem *audit trail* dan mempersulit proses identifikasi apabila terjadi perubahan data atau penyalahgunaan akses, karena tidak dapat dipastikan apa aktivitas yang dilakukan dan siapa pengguna sebenarnya di balik aktivitas tersebut (Wardani et al., 2024).

Selanjutnya, berdasarkan hasil observasi dan wawancara dengan petugas pendaftaran rawat jalan, diketahui bahwa sebagian petugas terbiasa menyimpan *username* dan *password* melalui fitur penyimpanan otomatis pada *browser*.



Gambar 1.2 *Username* dan *Password* Tersimpan di *Browser*

Hal tersebut dapat dilihat pada Gambar 1.2, yang menunjukkan *username* dan *password* tersimpan secara otomatis pada *browser* yaitu Google Chrome. Temuan ini diperkuat oleh pernyataan salah satu petugas pendaftaran rawat jalan sebagai berikut:

> "*Iya disimpan di browser. Oleh karena itu, pernah terjadi kasus petugas lain itu pake akunnya orang lain terus saat pengisian data kunjungan itu salah akhirnya yang disalahkan yang punya akun"*
>
> (Informan 4, 2025)

Hasil wawancara juga menunjukkan bahwa sebagian petugas memang terbiasa menyimpan *username* dan *password* pada fitur penyimpanan otomatis di *browser*. Kebiasaan ini pernah menimbulkan insiden ketika akun yang tersimpan tersebut diakses oleh pihak lain tanpa izin yang kemudian melakukan kesalahan dalam pengisian data kunjungan. Permasalahan ini menggambarkan kelemahan dalam aspek *integrity*, karena aspek ini menekankan bahwa setiap

perubahan informasi dalam sistem harus dilakukan oleh pengguna yang berwenang dan dapat diketahui oleh sistem yang ada (Sofia et al., 2022).

Untuk memastikan keamanan rekam medis elektronik tetap terjaga, penerapannya harus mengacu pada prinsip-prinsip keamanan data dan informasi yang tercantum dalam Peraturan Menteri Kesehatan Nomor 24 Tahun 2022. Regulasi tersebut menegaskan bahwa penyelenggaraan rekam medis elektronik wajib memenuhi tiga prinsip utama keamanan data dan informasi, yaitu kerahasiaan (*Confidentiality)*, integritas (*Integrity)*, dan ketersediaan (*Availability)*. Dengan memenuhi prinsip-prinsip tersebut, fasilitas pelayanan kesehatan dapat menjaga keamanan rekam medis elektronik secara lebih optimal.

Berdasarkan latar belakang yang telah diuraikan, serta mempertimbangkan pentingnya peran Rumah Sakit Tingkat III Baladhika Husada Jember dalam menjaga keamanan data pasien melalui rekam medis elektronik, maka diperlukan analisis keamanan rekam medis elektronik secara sistematis. Penelitian ini dibatasi pada penggunaan Rekam Medis Elektronik di instalasi rawat jalan, karena temuan permasalahan awal dan proses penggalian data yang dilakukan peneliti berada pada instalasi tersebut. Untuk itu, peneliti tertarik untuk melakukan penelitian dengan judul "Analisis Keamanan Rekam Medis Elektronik Instalasi Rawat Jalan Berdasarkan Aspek *Confidentiality, Integrity,* dan *Availability* di Rumah Sakit Tingkat III Baladhika Husada Jember".

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka dirumuskan permasalahan yaitu "Bagaimana analisis keamanan rekam medis elektronik instalasi rawat jalan berdasarkan aspek *confidentiality, integrity,* dan *availability* di Rumah Sakit Tingkat III Baladhika Husada Jember?"

1.3 Tujuan Penelitian

1.3.1 Tujuan Umum

Untuk menganalisis keamanan rekam medis elektronik instalasi rawat jalan berdasarkan aspek *confidentiality, integrity,* dan *availability* di Rumah Sakit Tingkat III Baladhika Husada Jember.

1.3.2 Tujuan Khusus

a. Menganalisis keamanan rekam medis elektronik instalasi rawat jalan di Rumah Sakit Tingkat III Baladhika Husada Jember berdasarkan aspek *Confidentiality* (Kerahasiaan*)*.
b. Menganalisis keamanan rekam medis elektronik instalasi rawat jalan di Rumah Sakit Tingkat III Baladhika Husada Jember berdasarkan aspek *Integrity* (Integritas*)*.
c. Menganalisis keamanan rekam medis elektronik instalasi rawat jalan di Rumah Sakit Tingkat III Baladhika Husada Jember berdasarkan aspek *Availability* (Ketersediaan*)*.
d. Menganalisis prioritas masalah keamanan rekam medis elektronik instalasi rawat jalan di Rumah Sakit Tingkat III Baladhika Husada Jember dengan menggunakan metode USG (*Urgency, Seriousness, Growth*).
e. Menyusun upaya rekomendasi penyelesaian masalah terkait aspek keamanan rekam medis elektronik di Rumah Sakit Tingkat III Baladhika Husada Jember dengan menggunakan metode diskusi.

1.4 Manfaat Penelitian

1.4.1 Bagi Politeknik Negeri Jember

a. Menambah referensi Perpustakaan Politeknik Negeri Jember terkait standar teknis dan prosedur keamanan rekam medis elektronik.
b. Menambah wawasan mahasiswa tentang analisis keamanan rekam medis elektronik di institusi layanan kesehatan.
c. Sebagai referensi bagi mahasiswa yang akan melakukan penelitian selanjutnya.

1.4.2 Bagi Rumah Sakit Tingkat III Baladhika Husada Jember

a. Memberikan gambaran keamanan sistem rekam medis elektronik berdasarkan standar nasional.
b. Sebagai bahan masukan atau saran bagi rumah sakit dalam pengambilan kebijakan dan menjaga keamanan sistem rekam medis elektronik di Rumah Sakit Tingkat III Baladhika Husada Jember

1.4.3 Bagi Peneliti

1. Menambah wawasan dan pemahaman tentang standar keamanan sistem rekam medis elektronik.
2. Sebagai sarana untuk menerapkan ilmu yang diperoleh selama mengikuti perkuliahan, khususnya dalam menerapkan standar kompetensi PMIK terkait menjaga privasi, keamanan, dan kerahasiaan data dan informasi.