BAB I
PENDAHULUAN

A. Latar Belakang

Rekam medis elektronik (RME) merupakan sistem digital yang dirancang untuk mencatat dan mengelola informasi Kesehatan pasiensecara terintegrasi. Penggunaan RME memerlukan jaminan terhadap keamanan dan kerahasiaan data pasien. Keamanan data di sini mengacu pada langkah-langkah perlindungan untuk mencegah akses tidak sah terhadap informasi pasien.[1] Kebocoran data pada RME dapat menimbulkan berbagai dampak negatif, termasuk risiko penyalahgunaan informasi oleh pihak yang tidak bertanggung jawab. Meskipun RME memiliki potensi untuk meningkatkan mutu pelayanan kesehatan, penerapannya di fasilitas kesehatan seperti puskesmas, masih menghadapi berbagai kendala. Kurangnya sinkronisasi data antara sistem RME dengan sistem informasi lain berdampak pada keamanan data pasien.[2] Menimbulkan duplikasi data, kesulitan akses informasi pasien secara *real-time*, serta meningkatkan potensi terjadinya pelanggaran data dan penyalahgunaan informasi.

Pelanggaran keamanan dan integritas data dalam sistem RME tidak hanya berdampak pada aspek teknis dan operasional, tetapi juga memiliki konsekuensi hukum dan etika yang serius. Risiko kebocoran data dapat melanggar hak *privasi* pasien, berpotensi memicu tuntutan hukum, dan menimbulkan tantangan besar dalam upaya menjaga kepercayaan masyarakat.[3] Kurangnya fitur keamanan pada perangkat dapat membuka celah bagi penyerang untuk mengakses informasi sistem, melakukan manipulasi, atau mencuri data. Dalam konteks data pasien, kelemahan ini berpotensi membahayakan privasi, integritas, dan kerahasiaan informasi medis yang sangat penting. Dengan penerapan langkah-langkah keamanan data yang memadai, keberlangsungan operasional sistem rekam medis elektronik dapat terjamin, risiko serangan siber dapat diminimalkan, serta dampak kerugian akibat kebocoran data dapat diminimalisir.[4]

Menurut *Health Insurance Portability and Accountability* (HIPAA), keamanan informasi harus memenuhi sejumlah elemen penting. Pertama, memastikan bahwa informasi kesehatan tetap rahasia, terjamin integritas nya, dan selalu tersedia, serta melindungi seluruh proses pengelolaan informasi, mulai dari pembuatan, penerimaan, pemeliharaan, hingga transmisi. Kedua, melindungi informasi dari ancamandan risiko yang dapat diprediksi, mencegah penggunaan yang tidak semestinya, serta memastikan kepatuhan tenaga kerja terhadap aturan terkait privasi.[5] Berdasarkan Permenkes Nomor 24 Tahun 2022 Pasal 29 Pasal tersebut menegaskan bahwa kerahasiaan rekam medis merupakan upayaperlindungan terhadap data dan informasi, memastikan keamanan dari gangguan yang berasal dari pihak internal maupun eksternal yang tidak berwenang untuk mengaksesnya. Ketentuan ini memastikan bahwa data daninformasi dalam Rekam Medis Elektronik (RME) dilindungi dari penggunaan dan penyebaran yang tidak sah.[6] Aspek keamanan data dalamsistem informasi RME sering kali diabaikan, terutama dalam hal perlindungan data pasien. Padahal, keamanan data pribadi merupakan elemen kunci untuk menjaga kepercayaan pengguna dan mendukung efisiensi layanan kesehatan.[7]

Keamanan informasi data pasien mencakup beberapa aspek penting, yaitu kerahasiaan (*privacy*), integritas (*integrity*), ketersediaan (*availability*), kontrol akses (*access control*). *Privacy* merupakan upaya menjaga informasi dari akses pihak yang tidak berhak, terutama karena data rekam medis pasien merupakan dokumen rahasia yang wajib dilindungi.[8] Menurut Nurul Hayaty integritas data berarti memastikan bahwa informasi tetap asli dan tidak mengalami perubahan tanpa persetujuan pemiliknya. Perlindungan aspek-aspek tersebut menjadi pondasi dalam menciptakan sistem RME yang andal dan terpercaya.[9] Berdasarkan wawancara yang dilakukan di salah satu puskesmas yang menjadi sampel dari 22 puskesmas, petugas menyampaikan bahwa penerapan RME di puskesmas telah dilakukan sejak tahun 2023. Selama penerapan RME di Puskesmas, pernah terjadi kehilangan data pasien pada aplikasi e-Puskesmas yang disebabkan

kelalaian petugas. Selain itu, petugas juga mengungkapkan bahwa aspek keamanan perlu ditingkatkan, mengingat aplikasi e-Puskesmas saat ini masih dapat diakses dari mana saja. Idealnya, akses terhadap aplikasi tersebut dibatasi hanya di lingkungan puskesmas untuk mencegah potensi ancaman keamanan data.

Jika aspek keamanan ini tidak diperhatikan dengan baik, dampaknya dapat berupa kasus kebocoran dan pencurian data pasien, yang pada akhirnya dapat merugikan baik pihak pasien maupun fasilitas kesehatan. Seperti kasus ketidakamanan data pasien di Puskesmas Kota Cirebon yang menunjukkan perlunya penerapan sistem keamanan yang lebih ketat dalam pengelolaan data rekam medis elektronik. Oleh karena itu, perlindungan terhadap aspek kerahasiaan, integritas, dan kontrol akses harus menjadi prioritas utama dalam upaya pengembangan sistem RME di puskesmas maupun fasilitas kesehatan lainnya.

Ketersediaan data (*availability*) bertujuan memastikan bahwa hanya pihak yang memiliki kewenangan yang dapat mengakses informasi. Salah satu langkah untuk mendukung hal ini adalah dengan menerapkan sistem autentikasi, seperti penggunaan nama pengguna dan kata sandi pada aplikasi web, guna mencegah akses oleh pihak yang tidak berwenang.

Sementara itu[10] pengendalian akses *(access control*) berfungsi melindungi jaringan dari ancaman internal maupun eksternal, dengan mengontrol siapa yang bisa mengakses sistem, kapan bisa diakses, dan dari mana akses dilakukan.[11]

Berdasarkan penelitian sebelumnya, implementasi aspek keamanan informasi pada rekam medis elektronik masih tergolong rendah[12] . Meskipun telah ada penguatan regulasi melalui Permenkes Nomor 24 Tahun 2020 tentang Rekam Medis Elektronik, tingkat keamanan informasi di sejumlah fasilitas pelayanan kesehatan masih dinilai "tidak memadai". Oleh karena itu, penelitian dengan judul "Keamanan Informasi Data Pasien Pada Penerapan RME di Puskesmas Kota Cirebon dilakukan untuk menelaah lebih lanjut permasalahantersebut

B. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, peneliti merumuskan permasalahan penelitian sebagai berikut: "Bagaimana tingkat keamanan informasi data pasien dalam penerapan Rekam Medis Elektronik (RME) di Puskesmas Kota Cirebon?"

C. Tujuan Penelitian

1. Tujuan Umum

Mengetahui aspek keamanan data pasien dalam penerapan rekam medis elektronik di puskesmas Kota Cirebon

2. Tujuan Khusus

a. Menggambarkan aspek keamanan data pasien dalam penerapan rekam medis di Puskesmas Kota Cirebon berdasarkan aspek kerahasian (*privacy*)
b. Menggambarkan aspek keamanan data pasien dalam penerapan rekam medis di Puskesmas Kota Cirebon berdasarkan aspek integritas (*integrity*).
c. Menggambarkan aspek keamanan data pasien dalam penerapan rekam medis di Puskesmas Kota Cirebon berdasarkan aspek ketersediaan (*availability*).
d. Menggambarkan aspek keamanan data pasien dalam penerapan rekam medis di Puskesmas Kota Cirebon berdasarkan aspek akses kontrol (*access control*).

D. Manfaat Penelitian

1. Bagi Dinas Kesehatan

Penelitian ini bertujuan untuk menganalisis tingkat keamanan data pasien di Puskesmas Kota Cirebon, dengan harapan dapat menjadi rujukan atau bahan pertimbangan dalam meningkatkan perlindungan data pasien pada sistem rekam medis elektronik. Secara khusus, fokus penelitian ini adalah pada aspek keamanan data pasien di Puskesmas, yang memerlukan evaluasi mendalam dan perbaikan yang berkelanjutan. Diharapkan, hasil penelitian ini dapat menjadi pedoman

yang jelas untuk memperkuat perlindungan data pasien melalui penerapan standar keamananyang lebih ketat, pengambilan kebijakan yang relevan, dan pemanfaatan teknologi modern. Upaya ini bertujuan untuk menciptakan sistem pengelolaan data yang aman dan efisien.[13]

2. Bagi Instansi Pendidikan

   Penelitian ini diharapkan dapat menjadi referensi bagi penelitian-penelitian berikutnya yang berkaitan dengan topik serupa. Selain itu, hasil penelitian ini juga diharapkan dapat digunakan sebagai bahan pembelajaran dan pengembangan ilmu pengetahuan, khususnya bagi mahasiswa Jurusan Rekam Medis dan Informasi Kesehatan Poltekkes Kemenkes Tasikmalaya.

3. Bagi Peneliti

   Karya tulis ilmiah ini diharapkan dapat memberikan manfaat bagi institusi pendidikan, khususnya dalam hal pengembangan dan peningkatan ilmu pengetahuan serta keterampilan mahasiswa

E. Keaslian penelitian

Tabel 1. 1 Keaslian Penelitian

No	Penelitian	Judul Penelitian	Metode Penelitian	Variabel	Letak Variabel
1.	Siti Sofia, Efri Tri Ardianto, Niyalatul Muna, Sabran (2022)	Analisis Aspek Keamanan Informasi Pasien Pada Penerapan RME di Fasilitas Kesehatan	Metode penelitian *Literature Review*	*Privacy, integrity, authentication , availability, access control,* dan *non-repudiation*	Metode penelitian dan tempat penelitian
2.	Efri Tri Ardianto, Sabran, dan Lensa Nurjanah (2024)	Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik di Rumah Sakit X	Metode penelitian kualitatif dengan pengumpulan data melalui wawancara, observasi, dan dokumentasi	*Privacy, confidentiality , integrity, availability, non-repudiation, authentication , dan authorization*	Variabel penelitian dan tempat penelitian
3.	Diva	Aspek	Metode	*Privacy,*	Tempat

No	Penelitian	Judul Penelitian	Metode Penelitian	Variabel	Letak Variabel
	Rizky Amanda Tiorentap dan Hosizah (2020)	Keamanan Informasi Dalam Penerapan Rekam Medis Elektronik di Klinik Medical Check-Up MP	penelitian deskriptif kualitatif dengan pengumpulan data melalui observasi dan wawancara	*integrity, authentication, availability, access control, dan non-repudiation*	penelitian
4.	Dwi Novi Rahayu	Analisis Aspek Keamanan Informasi Rekam Medis Dalam Sistem Informasi Manajemen Rumah Sakit Terintegrasi (SINERGIS) Dalam Penerapan Rekam Medis Elektronik di RSUP dr. Soeradji Tirtonegoro Klaten	Metode penelitian kualitatif	*Confidentiality, integrity, authentication, availability, access control, dan non-repudiation*	Variabel penelitian dan tempat penelitian
5.	Endah Wardani, Daniel Happy Putra, Dina Sonia, Noor Yulia	Keamanan Sistem Informasi Rekam Medis Elektronik di Rumah Sakit Islam Jakarta Sukapura	Metode penelitian deskriptif kualitatif dengan 7 informan	*Privacy, integrity, authentication, availability, access control, dan non-repudiation*	Tempat penelitian