

BAB I

PENDAHULUAN

A. Latar Belakang

Era transformasi digital telah membawa perubahan signifikan dalam berbagai sektor, termasuk sektor kesehatan. Digitalisasi layanan kesehatan tidak hanya mengubah cara pemberian pelayanan, tetapi juga mengubah cara pengelolaan data dan informasi kesehatan. Pemanfaatan teknologi informasi dalam pelayanan kesehatan diharapkan dapat meningkatkan efisiensi, akurasi, serta kualitas layanan kesehatan kepada masyarakat. Transformasi digital dalam layanan kesehatan menjadi suatu keniscayaan yang harus diikuti oleh seluruh fasilitas pelayanan kesehatan guna meningkatkan mutu pelayanan dan daya saing di era modern (Cahyanti dkk., 2025).

Dalam rangka memperkuat pelayanan kesehatan tingkat pertama, Kementerian Kesehatan Republik Indonesia menerbitkan Peraturan Menteri Kesehatan Nomor 19 Tahun 2024 tentang Puskesmas. Peraturan ini menegaskan bahwa Puskesmas merupakan fasilitas pelayanan kesehatan tingkat pertama yang bertanggung jawab dalam penyelenggaraan upaya kesehatan masyarakat dan perseorangan dengan mengutamakan upaya promotif dan preventif untuk mencapai derajat kesehatan masyarakat yang setinggi-tingginya di wilayah kerjanya. Seiring dengan perkembangan teknologi, Puskesmas dituntut untuk menerapkan sistem informasi kesehatan yang terintegrasi guna mendukung efektivitas

pelayanan kesehatan kepada masyarakat (Kemenkes RI No. 43, 2019).

Di sisi lain, peralihan dari sistem manual ke sistem elektronik menimbulkan tantangan penting terkait keamanan data pasien. Rekam medis elektronik menyimpan informasi sensitif pasien yang harus dijaga kerahasiaannya sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. Fasilitas kesehatan memiliki kewajiban untuk memastikan perlindungan data pasien dari akses yang tidak sah, modifikasi tanpa izin, maupun kehilangan data. Apabila terjadi pelanggaran keamanan data, pasien dapat mengalami kerugian berupa pelanggaran privasi atau penyalahgunaan informasi medis yang dapat merugikan kepentingan pasien (UU No. 17, 2023).

Keamanan informasi dalam layanan kesehatan digital didasarkan pada tiga aspek utama yang disebut CIA Triad, yaitu *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan). Kerahasiaan memastikan bahwa data hanya dapat diakses oleh pihak yang memiliki kewenangan. Integritas menjamin bahwa data tidak mengalami modifikasi tanpa izin dan tetap akurat serta konsisten. Ketersediaan memastikan bahwa data dan sistem dapat digunakan setiap saat ketika dibutuhkan oleh pengguna yang berwenang. Ketiga aspek ini menjadi landasan penting dalam menilai apakah sistem informasi kesehatan telah memenuhi standar keamanan yang diperlukan untuk melindungi data pasien (Harahap dkk., 2023).

Puskesmas Danurejan II telah menerapkan Rekam Medis Elektronik (RME) secara penuh sejak tahun 2023 dengan menggunakan aplikasi SIMPUS. Sebelumnya, penerapan rekam medis dilakukan secara *hybrid*, yaitu pencatatan data pasien masih dilakukan secara manual pada beberapa tahap pelayanan, kemudian diinput kembali ke dalam sistem oleh petugas rekam medis. Kondisi ini terjadi karena keterbatasan jumlah tenaga serta tingginya jumlah kunjungan pasien setiap harinya. Penerapan SIMPUS secara penuh tentu memberikan banyak manfaat dalam meningkatkan efisiensi dan kualitas pelayanan kesehatan. Namun, di sisi lain, penggunaan sistem elektronik juga menuntut adanya jaminan keamanan data yang lebih kuat, mengingat rekam medis memuat informasi pasien yang bersifat sangat rahasia.

Berdasarkan hasil studi pendahuluan, masih ditemukan beberapa permasalahan yang berkaitan dengan aspek keamanan data pada aplikasi SIMPUS. Hingga saat ini, belum pernah dilakukan evaluasi terkait keamanan data pada aplikasi SIMPUS, sehingga potensi risiko keamanan belum teridentifikasi dan terdokumentasi secara menyeluruh. Salah satu permasalahan yang ditemukan adalah belum diterapkannya standar kompleksitas kata sandi yang ideal, di mana sistem belum mewajibkan penggunaan kombinasi huruf kapital, huruf kecil, angka, dan simbol, serta belum menetapkan batas minimal panjang karakter. Selain itu, belum terdapat kebijakan pembaruan kata sandi secara berkala, sehingga berpotensi meningkatkan risiko kebocoran data dan akses tidak sah

terhadap informasi rekam medis pasien.

Pada aspek *Confidentiality* (kerahasiaan), masih ditemukan kebiasaan petugas yang saling meminjamkan akun pengguna SIMPUS. Kebiasaan ini berpotensi menimbulkan penyalahgunaan hak akses serta menyulitkan proses penelusuran tanggung jawab apabila terjadi pelanggaran keamanan data. Pada aspek *Integrity* (integritas), terdapat keterbatasan pada tampilan menu pencatatan diagnosis dokter dalam SIMPUS, di mana sistem belum menyediakan pemisahan yang jelas antara diagnosis utama dan diagnosis sekunder, serta terdapat pengulangan kolom diagnosis dokter. Kondisi tersebut berpotensi menimbulkan kesalahan input data dan dapat mempengaruhi keakuratan informasi rekam medis elektronik. Pada aspek *Availability* (ketersediaan), keterbatasan perangkat komputer yang tersedia juga menjadi kendala dalam penggunaan SIMPUS secara optimal. Kondisi ini dapat mempengaruhi kelancaran pelayanan kesehatan, terutama pada saat banyak petugas membutuhkan akses sistem secara bersamaan.

Selain permasalahan teknis, proses implementasi SIMPUS di Puskesmas Danurejan II belum sepenuhnya didukung oleh adanya program pelatihan atau pengenalan resmi bagi pegawai baru. Dokumen pedoman atau *manual book* penggunaan SIMPUS yang tersedia merupakan dokumen lama yang disusun pada tahun 2005, yaitu pada saat SIMPUS pertama kali diterapkan, dan hingga saat ini belum pernah dilakukan revisi atau pembaruan. Kondisi tersebut menyebabkan pedoman penggunaan

yang ada belum sepenuhnya menyesuaikan dengan perkembangan sistem, kebutuhan pengguna, serta kebijakan keamanan data terkini. Akibatnya, sebagian besar pegawai mempelajari penggunaan SIMPUS secara mandiri serta melalui berbagi informasi antar rekan kerja, yang berpotensi menimbulkan perbedaan pemahaman dalam penggunaan sistem serta meningkatkan risiko kesalahan dalam pengelolaan data.

Berdasarkan kondisi tersebut, dapat disimpulkan bahwa meskipun SIMPUS telah diterapkan secara penuh dalam mendukung pengelolaan Rekam Medis Elektronik, aspek keamanan data yang meliputi *confidentiality*, *integrity*, dan *availability* belum pernah dievaluasi secara khusus dan menyeluruh, serta belum didukung oleh pedoman penggunaan yang mutakhir. Oleh karena itu, penelitian mengenai “Tinjauan Keamanan Data Rekam Medis Elektronik pada Aplikasi SIMPUS Berdasarkan Aspek *Confidentiality*, *Integrity*, dan *Availability* (CIA) di Puskesmas Danurejan II” menjadi penting untuk dilakukan sebagai upaya memberikan gambaran nyata mengenai kondisi keamanan data serta sebagai dasar penyusunan rekomendasi perbaikan sistem dan pedoman penggunaan di masa mendatang.

B. Rumusan Masalah

Bagaimana keamanan data Rekam Medis Elektronik pada aplikasi SIMPUS berdasarkan aspek *confidentiality*, *integrity*, dan *availability* di Puskesmas Danurejan II?

C. Tujuan Penelitian

1. Tujuan Umum

Mengetahui keamanan data Rekam Medis Elektronik pada aplikasi SIMPUS di Puskesmas Danurejan II.

2. Tujuan Khusus

a. Mengetahui keamanan data SIMPUS berdasarkan aspek *confidentiality* di Puskesmas Danurejan II

b. Mengetahui keamanan data SIMPUS berdasarkan aspek *integrity* di Puskesmas Danurejan II

c. Mengetahui keamanan data SIMPUS berdasarkan aspek *availability* di Puskesmas Danurejan II.

D. Ruang Lingkup

Penelitian ini dilakukan di Puskesmas Danurejan II Kota Yogyakarta dengan fokus pada pengguna aplikasi SIMPUS. Subjek penelitian meliputi petugas rekam medis dan pengguna aplikasi SIMPUS yang terdiri dari petugas pendaftaran, dokter umum, perawat, petugas laboratorium, dan petugas farmasi. Penelitian ini mengkaji aspek keamanan data berdasarkan tiga pilar *CIA Triad: confidentiality, integrity, dan availability*. Penelitian ini tidak mencakup pengembangan sistem baru maupun analisis biaya investasi teknologi keamanan.

E. Manfaat Penelitian

1. Manfaat Teoritis

Penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan keilmuan di bidang Manajemen Informasi Kesehatan, khususnya terkait keamanan data rekam medis elektronik. Hasil penelitian ini dapat memperkaya kajian teoritis mengenai penerapan aspek *Confidentiality*, *Integrity*, dan *Availability* dalam sistem informasi kesehatan, serta menjadi referensi bagi penelitian selanjutnya yang membahas keamanan data pada sistem informasi kesehatan, khususnya aplikasi SIMPUS di fasilitas pelayanan kesehatan tingkat pertama.

2. Manfaat Praktis:

a. Bagi Puskesmas, penelitian ini diharapkan dapat memberikan gambaran objektif tentang tingkat keamanan data rekam medis elektronik yang saat ini diterapkan di Puskesmas Danurejan II. Hasil penelitian ini dapat menjadi dasar untuk melakukan perbaikan sistem keamanan data yang lebih komprehensif sehingga dapat meningkatkan kepercayaan pasien terhadap keamanan data pribadi mereka yang tersimpan dalam sistem.

b. Bagi Institusi Poltekkes Kemenkes Yogyakarta, penelitian ini diharapkan dapat menambah referensi penelitian tentang keamanan data rekam medis elektronik khususnya pada aplikasi SIMPUS. Penelitian ini juga memberikan gambaran praktis mengenai

implementasi sistem informasi kesehatan di lapangan yang dapat menjadi bahan pembelajaran untuk mahasiswa program studi Rekam Medis dan Informasi Kesehatan dalam memahami pentingnya aspek keamanan data dalam sistem informasi kesehatan.

- c. Bagi peneliti, penelitian ini bermanfaat untuk menambah pengetahuan dan pemahaman penulis tentang keamanan sistem informasi kesehatan serta dapat mengaplikasikan teori keamanan informasi dalam konteks pelayanan kesehatan secara langsung. Selain itu, penelitian ini juga dapat meningkatkan kompetensi penulis dalam melakukan evaluasi sistem informasi yang dapat diterapkan di dunia kerja.

F. Keaslian Penelitian

Tabel 1. Keaslian Penelitian

No	Nama Peneliti	Judul	Metode Penelitian	Hasil Penelitian	Persamaan dan Perbedaan
1	(Agustin Nanik dan Setiyani Imaniar, 2020)	Tinjauan Keamanan SIM-PUS Berdas-arkan Aspek <i>Confidentiality</i> , <i>Integrity</i> , dan <i>Availability</i> di Puskesmas Gamping 1	Penelitian kua-litatif metode deskriptif, data dikumpulkan melalui waw-ancara, observ-asi, dan doku-mentasi.	<i>Confidentiality</i> , <i>Integrity</i> , dan <i>Availability</i> pada SIMPUS sudah diterapkan, nam-un masih terda-pat kendala sepe-rti pengelolaan <i>password</i> , peng-awasan peruba-han data, serta gangguan sistem /jaringan.	Persamaan: Sama-sama me-neliti keamanan SIMPUS berdas-arkan <i>CIA</i> deng-an metode kual-i-tatif. Perbedaan: kondisi penerap-an keamanan di-sesuaikan dengan situasi di tempat penelitian masin-g-masing.
2	(Dinarsa-ri, Afin 2023)	Analisis Kea-manan Data Pada Penera-pan Rekam	Penelitian kua-litatif deskriptif melalui wawa-ncara, observa-	Keamanan data RME ditinjau dari beberapa aspek. <i>Availabil-</i>	Persamaan: Sama-sama men-eliti keamanan data RME/SIM-

No	Nama Peneliti	Judul	Metode Penelitian	Hasil Penelitian	Persamaan dan Perbedaan
		Medis Elektronik di RSUD Dr. Adhyatma, MPH Provinsi Jawa Tengah	si, dan dokumentasi.	ity sudah berjalan baik, namun masih terdapat kelemahan pada <i>confidentiality</i> , <i>integrity</i> , <i>authentication</i> , <i>access control</i> , dan <i>non-repudiation</i> .	PUS berdasarkan prinsip keamanan informasi. Perbedaan: Lokasi dan sistem yang diteliti berbeda, serta cakupan aspek keamanan yang digunakan.
3	(Qothrunada, R. I. 2023)	Analisis Keamanan Sistem Informasi Manajemen Terintegrasi RSUP Dr. Sardjito (SIME-TRISS) Berdasarkan Aspek <i>Privacy</i> , <i>Integrity</i> , dan <i>Authentication</i>	Penelitian kualitatif deskriptif dengan teknik wawancara dan observasi.	Ditemukan masih terdapat celah keamanan pada aspek <i>privacy</i> , <i>integrity</i> , dan <i>authentication</i> , seperti penggunaan akun bersama dan pembatasan hak akses yang belum optimal	Persamaan: Sama-sama meneliti keamanan sistem informasi kesehatan dengan pendekatan kualitatif. Perbedaan: Sistem dan aspek keamanan yang digunakan berbeda dengan penelitian yang diajukan.
4	(Suhariyono, Rusdianikawati dan Afifah, 2025)	Analisis Aspek Keamanan Informasi Data Pasien pada Rekam Medis Elektronik di UPT Puskesmas Karangploso	Observasi dan wawancara dengan pendekatan deskriptif	Terdapat kelemahan pada kontrol akses (<i>confidentiality</i>), <i>backup (integrity)</i> , dan sistem <i>down (availability)</i> . Disarankan peningkatan kontrol akses dan sistem pencadangan.	Persamaan: Sama-sama menggunakan kerangka CIA pada sistem puskesmas. Perbedaan: Menggunakan E-puskesmas bukan SIMPUS.
5	(Prabawati dkk., 2023)	Tinjauan Keamanan Data Rekam Medis Elektronik Di Puskesmas Jabung	Penelitian deskriptif kualitatif melalui observasi dan wawancara	Terdapat kelemahan pada aspek <i>confidentiality</i> (akses belum optimal), <i>integrity (backup</i> tidak rutin), dan <i>availability</i> (sistem sering <i>down</i>)	Persamaan: Menggunakan kerangka CIA pada sistem rekam medis elektronik di puskesmas. Perbedaan: penelitian sebelumnya menilai keamanan sistem secara umum belum berdasarkan peran petugas
6	(Widiyanti, Hastuti dan kusumaw	Tinjauan Keamanan Data Rekam Medis Elektronik	Deskriptif kualitatif melalui observasi dan wawancara pa-	Ditemukan kelemahan pada fitur keamanan, seperti tidak adanya	Persamaan: Sama-sama meneliti aspek CIA pada SIMPUS.

No	Nama Peneliti	Judul	Metode Penelitian	Hasil Penelitian	Persamaan dan Perbedaan
	ati, 2024)	Pada Aplikasi Simpus Berdasarkan Aspek <i>Confidentiality</i> , <i>Integrity</i> , Dan <i>Availability</i> Di Puskesmas Tasikmadu Karanganyar	da beberapa puskesmas pengguna SIMPUS	<i>logout</i> otomatis dan manajemen akses belum optimal	Perbedaan: Penelitian sebelumnya hanya meninjau keamanan data SIMPUS pada bagian pendaftaran rawat jalan.