BAB I
PENDAHULUAN

A. Latar Belakang

Berdasarkan Undang-Undang RI No. 17 tahun 2023 tentang kesehatan, fasilitas pelayanan kesehatan digunakan untuk meneyediakan layanan kesehatan kepada individu dan masyarakat dengan pendekatan promotif, preventif, kuratif, rehabilitatif, dan paliatif yang diselenggarakan oleh pemerintahan pusat, daerah, dan masyarakat. Fasilitas lengkap ini guna mendukung keberhasilan dalam suatu pelayanan kesehatan yang paripurna salah satunya pada fasilitas kesehatan pelayanan di rumah sakit, rekam medis yang sekarang dikenal sebagai Rekam Medis Elektronik merupakan bentuk pemanfaatan sistem informasi.

Dalam teknologi informasi dan komunikasi yang berkembang pesat saat ini ,perkembangan teknologi informasi dan komunikasi, rumah sakit semakin banyak menerapkan teknologi untuk meningkatkan efisiensi dan kualitas pelayanan medis. Mengembangkan Teknologi Informasi Komunikasi (TIK) memiliki peran yang sangat penting dalam mendukung kehidupan sehari-hari, salah satunya pada bidang kesehatan (Rosadi, 2016). Menurut Permenkes Nomor 18 tahun 2022, bahwa sistem informasi kesehatan adalah seperangkat tatanan yang meliputi data, informasi, indikator, prosedur, perangkat, teknologi, dan sumber daya manusia yang saling berkaitan dan dikelola secara terpadu untuk mengarahkan tindakan atau keputusan yang berguna dalam mendukung pembangunan kesehatan.

Penggunaan (RME) menjadi satu contoh implementasi teknologis bertujuan untuk meningkatkan efisiensi dan akurasi data medis, memfasilitasi kolaborasi tim medis, memperbaiki proses pengambilan keputusan klinis, mengurangi kesalahan medis dan risiko pasien (Siswati et al., 2024). Adanya perkembangan teknologi informasi komunikasi terlihat signifikan dalam pengelolaan rekam medis dari metode tradisional ke sistem digital. Sistem

administrasi dokumen berbasis komputer atau elektronik yang tengah menjadi tren di seluruh dunia dalam dunia kesehatan sekarang ini yaitu RME. Berdasarkan PMK No. 24 tahun 2022 Tentang Rekam Medis, ini merupakan dokumen yang mencatat informasi identitas pasien, riwayat pemeriksaan, pengobatan, tindakan medis, dan layanan lain yang diberikan kepada pasien. Rekam Medis Elektronik (RME) adalah versi rekam medis yang dibuat dengan menggunakan sistem elektronik untuk memfasilitasi penyelenggaraan rekam medis. Salah satu aspek penting yang perlu diperhatikan. Salah satu hal yang harus diperhatikan dalam implementasi RME adalah keamanan informasi, sesuai dengan regulasi yang tercantum PMK No. 24 tahun 2022, pada pasal 29 ayat (1) harus mematuhi prinsip kemanan data RME, yang mencangkup aspek kerhasian, Integritas selalu menjaga keutuhan data, dan memastikan data selalu tersedia.

Pentingnya menjaga keamanan data yaitu untuk melindungi privasi individu, mencegah akses tidak sah, manipulasi, atau pencurian informasi sensitif, memastikan kepatuhan terhadap peraturan hukum, dan membangun kepercayaan publik dalam pengelolaan data (Dinarti et al., 2024). Keamanan data dapat melindungi privasi pasien dengan memastikan bahwa informasi kesehatan sensitif hanya dapat diakses oleh individu berwenang. Selain itu, kepatuhan terhadap regulasi dan peraturan yang berlaku, seperti Permenkes No. 24 Tahun 2022 di Indonesia, menjadi lebih mudah dipenuhi. Dengan mengurangi risiko serangan *cyber* dan kerusakan data, fasilitas pelayanan kesehatan dapat meningkatkan efisiensi operasional, sehingga kulitas layanan yang di berikan kepada pasien meningkat. Selain itu, pembangunan kepercayaan publik juga didorong, memungkinkan fasilitas kesehatan untuk menarik lebih banyak pasien dan memperkuat posisi mereka dalam industri pelayanan kesehatan. Meskipun manfaat keamanan data banyak, implementasinya seringkali sulit karena kompleksitas serta berbagai masalah yang terkait dengan keamanan data itu sendiri. Keamanan data pada sistem informasi kesehatan menghadapi beberapa masalah serius, terutama terkait pengelolaan server dan perlindungan data. Terkadang server tidak dikelola

dengan benar, sehingga data *backup* bisa hilang, dan serangan virus serta *hacker* menjadi ancaman nyata. Praktik pertukaran *username* dan *password* antar petugas rekam medis yang menggunakan NIK sebagai identifikasi meningkatkan risiko kebocoran data pasien. Selain itu, tidak adanya fitur *logout* otomatis memperburuk situasi ini. Prosedur reset *password* yang dilakukan oleh bagian IT, meskipun mereka tidak berwenang, serta kebijakan penggantian *password* setiap 120 (seratus dua puluh) hari yang sering menimbulkan masalah saat login, juga menambah kompleksitas keamanan. Untuk melindungi data BPJS, penting untuk mengimplementasikan langkah-langkah seperti penggunaan autentikasi dua faktor, prosedur reset password yang tepat, pengelolaan server yang baik, perlindungan dari serangan virus dan hacker, serta peninjauan hak akses secara berkala sesuai dengan PMK No 24 Tahun 2022.

Hal ini menunjukkan bahwa masalah keamanan data menjadi semakin serius karena tren pencurian data menjadi meningkat. Di Indonesia, kasus pencurian data kesehatan bukan hal yang baru. Pada tahun 2020, data 230 ribu pasien COVID-19 di Indonesia diduga telah dicuri dan dijual. Hal ini menyebabkan kerugian tidak hanya materil tetapi juga psikis korban, dimana mereka bisa saja mendapatkan perlakuan diskriminasi di lingkungan masyarakat. Pada bulan januari tahun 2022, terdapat juga dugaan kebocoran data catatan medis pasien di sejumlah rumah sakit di Indonesia. data berukuran 720 GB itu dijual di forum *online raidforums* (Sofia et al., 2022). Privasi pasien dan keamanan data yang dilakukan oleh Ponemon Institute dan diterbitkan pada bulan Desember 2012 menemukan bahwa 94% rumah sakit pernah mengalami pelanggaran privasi, dan 45% mengalami lebih dari lima pelanggaran. Pada suatu waktu, tercatat 21.210.439 orang menjadi korban pelanggaran pelayanan kesehatan; 1,85 juta korban pada tahun 2012 saja. Dapat dimengerti bahwa masyarakat semakin khawatir tentang privasi informasi kesehatan mereka (Herold and Beaver, 2015).

Kasus yang berhubungan dengan keamanan dan kerahasiaan data menjadi sangat krusial karena adanya pencurian data yang terus melonjak

seiring berjalannya waktu (Pradita et all, 2022). Berdasarkan penelitian (Tiorentap & Hosizah, 2020). Pada Klinik Medical *Check-Up* ditemukan bahwa terdapat ketidaksesuaian prinsip keamanan sistem informasi yakni antar user masih saling bertukar informasi terkait *user id* dan *password-nya.* Selain itu, satu *user-id* digunakan oleh beberapa orang juga sangat biasa dilakukan. Hal tersebut tidak sesuai dengan aspek *access control* dimana aspek tersebut menekankan pada cara pengaturan pembatasan hak akses terhadap informasi. Hal ini tentu saja akan berakibat fatal jika terjadi kesalahan penginputan, dimana menyulitkan untuk proses identifikasi pelaku. Jika hal tersebut terus berlanjut, dikhawatirkan akan mengakibatkan pada penggunaan informasi oleh pihak-pihak yang tidak bertanggung jawab. Penelitian yang dilakukan oleh (Nugraheni, 2018), diperoleh hasil sebagai berikut, aspek kerahasiaan (*privacy*) dapat dibuktikan dengan penjagaan informasi dari pihak yang tidak memiliki hak akses melalui *username* dan *password* bagi tiap pengguna, aspek integritas (*integrity*) dibuktikan dengan penghapusan data belum dapat terfasilitasi, aspek autentikasi (*authentication*) dibuktikan dengan akses terhadap informasi menggunakan *Personal Identification Number* (PIN), aspek ketersediaan (*availability*) dapat terfasilitasi namun belum maksimal, aspek kontrol akses (*access control*) terfasilitasi dengan adanya keterbatasan hak akses pengguna, aspek (*non repudiation*) dibuktikan dengan identifikasi terhadap pihak yang melakukan pengisian dan perubahan informasi belum maksimal. Merujuk pada kasus peretasan data yang terjadi, rumah sakit penyelenggara RME harus memenuhi aspek keamanan. Prinsip keamanan data informasi khususnya dalam bidang kesehatan. mencakup tiga aspek yaitu kerahasiaan, integritas, dan ketersediaan (Permenkes No. 24, 2022).

Menurut PMK No 24 Tahun 2024 RME harus mematuhi prinsip keamanan data dan informasi, termasuk kerahasiaan, yang merupakan jaminan keamanan data informasi dari campur tangan pihak internal dan eksternal yang tidak mempunyai akses, sehingga penggunaan dan distribusi data dan informasi yang terkandung dalam RME dilindungi. Integritas merupakan jaminan keakuratan data dan informasi yang terdapat dalam RME, dan

perubahan terhadap data hanya dapat dilakukan oleh orang yang diberikan hak akses untuk mengubahnya. *Availability* merupakan jaminan bahwa data dan informasi yang terdapat dalam RME dapat diakses dan digunakan oleh masyarakat yang mempunyai hak akses yang ditentukan oleh Kepala Fasilitas Pelayanan Kesehatan.

Menurut hasil studi awal yang dilaksanakan pada tanggal 27 Mei 2024 mengenai Implementasi RME di RS Panti Rapih Yogyakarta, ditemukan beberapa kendala yang terkait dengan keamanan sistem informasi. Salah satunya adalah praktik pertukaran informasi *username* dan *password* antar petugas rekam medis, yang menggunakan NIK sebagai identifikasi. Hal ini menyebabkan potensi kebocoran informasi data pasien jika setiap petugas masih sering bertukar nama pengguna dan kata sandi Sistem RS Panti Rapih Yogyakarta, belum punya fitur *logout* otomatis buat dokter dan petugas rekam medis kalau sistem ini penting dalam kemanan data di RS Panti Rapih Yogyakarta, karena hal ini dapat meningkatkan risiko akses tidak sah ke sistem. Lebih lanjut, ketika petugas lupa *password*, proses reset. dilakukan oleh bagian IT, meskipun sebenarnya bagian IT tidak memiliki kewenangan untuk mengganti *password* petugas. *Username* dan *password* biasanya ditetapkan oleh pihak SDM menggunakan NIK. Jika *password* lupa, petugas akan diminta untuk menggantinya dengan menggunakan GPS atau perangkat lunak lainnya yang memungkinkan mereka masuk ke sistem dan mengubah *password* dengan menggunakan kode OTP. Namun, jika petugas lupa *password* setelah menggantinya, proses reset harus dilakukan kembali dengan memasukkan NIK saat *login* ke aplikasi SIMRS dan mengganti *password* sesuai keinginan.

Selain itu, sistem menerapkan kebijakan agar *password* diubah setiap 120 (seratus dua puluh) hari untuk meningkatkan keamanan. Jika *password* telah digunakan selama 120 (seratus dua puluh) hari, petugas akan diminta untuk memperbarui *password* saat *login*. Namun, masih terjadi masalah di mana setelah mengganti *password,* ketika *login* kembali, terjadi kesulitan karena memasukkan *password* lama dan memasukkan *password* baru yang

tidak cocok. Terakhir, terkait hak akses, keputusan ditentukan oleh atasan dan dapat diminta untuk menambahkan atau mengurangi hak akses bagi seorang staf. Meskipun sistem RME telah diterapkan sejak tahun 2010 dan telah menggunakan standar keamanan ISO 27001 serta telah diaudit oleh BPJS di bidang IT, masih terdapat beberapa kelemahan yang perlu diperbaiki untuk meningkatkan keamanan dan efisiensi sistem.

Menurut Latar Belakang tersebut, peneliti berminat untuk melanjutkan penelitian tentang penerapan kemanan RME dengan mengangkat judul "Evaluasi Aspek Keamanan RME di Rumah Sakit Panti Rapih Yogyakarta".

B. Rumusan Masalah

Menurut latar belakang di atas, maka peneliti tertarik untuk merumuskan masalah, bagaimana penerapan aspek keamanan RME di Rumah Sakit Panti Rapih Yogyakarta.

C. Tujuan Penelitian

Tujuan penelitian ini terbagi menjadi dua, yaitu :

1. Tujuan Umum

   Mengevaluasi keamanan data dalam penerapan RME di Rumah Sakit Panti Rapih Yogyakarta.

2. Tujuan Khusus

   a. Mengidentifikasi penerapan aspek *privacy* pada RME di Rumah Sakit Panti Rapih Yogyakarta.

   b. Mengidentifikasi penerapan aspek *integrity* pada RME di Rumah Sakit Panti Rapih Yogyakarta.

   c. Mengidentifikasi penerapan aspek *availibility* pada RME di Rumah Sakit Panti Rapih Yogyakarta.

D. Manfaat Penelitian

Manfaat penyusun Karya Tulis Ilmiah merupakan manfaat yang diharapkan dari hasil penelitian antara lain :

1. Manfaat teoretis
   a. Bagi Pendidikan

      Dapat digunakan sebagai referensi untuk penelitian lebih lanjut dan untuk menambah materi perkuliahan tentang penerapan aspek keamanan Rekam Medis Elektronik (RME).
2. Manfaat praktis
   a. Bagi Rumah Sakit

      Sebagai bahan masukan dan evaluasi bagi rumah sakit dan unit kerja rekam medis, khususnya dalam evaluasi penerapan aspek keamanan RME di Rumah Sakit Panti Rapih Yogyakarta.
   b. Bagi Peneliti

      Dapat mengaplikasikan dan mengembangkan teori yang telah didapatkan selama proses belajar mengajar.
   c. Bagi Pendidikan

      Dapat digunakan sebagai referensi untuk penelitian lebih lanjut dan untuk menambah materi perkuliahan tentang penerapan aspek kemananan RME.

E. Keasliaan Penelitian

Tabel 1 1 Keaslian Penelitian

No	Nama	Judul Penelitian	Teknik Penelitian	Hasil	Perbedaan
1	(Sofia et al., 2022)	Analisis aspek keamanan informasi pasien pada penerapan RME di Fasilitas pelayanan Kesehatan	Literature review	Hasil tinjauan dari artikel didapatkan 6 (enam) aspek keamanan yakni *user* dan *password*, terdapatnya tanda tangan elektronik, perubahan maupun penghapusan data oleh administrator, aspek pemanfaatan proses pencadangan sebagai antisipasi	Metode penelitian, lokasi penelitian dan waktu penelitian.

2	(We'e et al., 2023)	Evaluasi Aspek Keamanan Dan Kerahasian RME Di Rumah Sakit Panti Nugroho	Penelitian ini menggunakan Deskripsi Kualitatif	Hasil Penelitian adalah penerapan aspek kerahasiaan dan keamanan RME , telah berjalan dengan baik. Unit Sistem Informasi Rumah Sakit telah menerapkan pemberian *user ide* beserta *password* pada setiap petugas kesehatan dan memberlakukan hak kewenangan dalam mengakses data rekam medis pasien untuk menjamin kerahasiaan dalam penggunaan RME . Penerapan sistem RME dapat meningkatkan efisiensi waktu, tenaga, dan biaya.	Perbedaan Lokasi penelitian dan Informan penelitian.
3	(Pradita et al., 2022)	Pentingnya Aspek Keamanan Data Pasien Pada Penerapan RME Di Puskesmas	Penelitian ini menggunakan Deskripsi Kualitatif	Kemanan Data Kesehatan dan informasi dalam penyelenggaraan RME yang sesuai dengan PMK 24 Tahun 2022 yaitu kerahasian,integritas, dan ketersedian.	Perbedaan Lokasi penelitian dan Informan penelitian.