BAB 1. PENDAHULUAN

1.1 Latar belakang

Perkembangan teknologi dan sistem informasi di dunia khsusunya di Indonesia semakin pesat dan menjangkau hampir seluruh bidang, termasuk bidang kesehatan. Pemanfaatan teknologi informasi pelayanan kesehatan dalam sektor pelayanan kesehatan di Indonesia menunjukkan perkembangan yang signifikan (Ningtyas & Lubis, 2018). Salah satunya adalah membangun sistem informasi pada bidang kesehatan dengan menyediakan fitur-fitur pelayanan kesehatan. Sistem informasi pada layanan kesehatan memberikan banyak keuntungan pemberi pelayanan yang dalam hal ini adalah rumah sakit, klinik, puskesmas, dan sebagainya.

Menurut Peraturan Pemerintah RI No 47 tahun 2016 Fasilitas Kesehatan adalah suatu alat dan/atau tempat yang digunkan untuk menyelenggarakan upaya pelayanan kesehatan, baik promotif, preventif, kuratif maupun rehabilitatif yang dilakukan oleh pemerintah pusat, pemerintah derah, dan/atau masyarakat. Setiap lokasi yang menyediakan pelayanana kesehatan, mulai dari klinik kecil, puskesmas hingga rumah sakit yang besar dengan fasilitas yang lengkap. Salah satu dokumen yang penting dalam fasilitas kesehatan disebut dengan dokumen rekam medis.

Suatu berkas yang berisikan catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang diberikan kepada pasien pada suatu fasilitas kesehatan merupakan suatu dokumen yang disebut dengan rekam medis.(Kemenkes, 2008). Berdasarkan Undang-Undang No 29 Tahun 2004 Tentang Praktik Kedokteran bahwa Rekam medis wajib disimpan dan dijaga kerahasiaannya oleh dokter atau dokter gigi dan pimpinan sarana layanan kesehatan. Pencatatan rekam medis wajib bagi dokter dan dokter gigi yang melakukan tindakan medis kepada pasien. (Kemenkes, 2008). Berdasarkan pada peraturan tersebut sehingga tidak ada alasan bagi dokter atau dokter gigi untuk tidak membuat rekam medik pasien.

Salah satu penerapan Teknologi Informasi (TI) di Indonesia pada bidang kesehatan disebut dengan Rekam Medik Elektronik (RME). RME telah banyak digunakan pada sistem informasi rumah sakit di Indonesia sebagai pengganti atau pelengkap rekam medik kesehatan berbentuk kertas. Sarana pelayanan kesehatan dapat menyelenggarakan rekam medik elektronik sesuai dengan Permenkes No 269 tahun 2008 bahwa Penyelenggaraan rekam medik dengan menggunakan teknologi informasi elektronik diatur lebih lanjut dengan peraturan tersendiri. Hal ini didukung oleh UU RI No 11 tahun 2008 tentang ITE bahwa suatu informasi harus berbentuk tertulis atau asli, informasi elektronik dan atau dokumen elektronik dikatakan sah jika informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Salah satu permasalahan besar jika dikaitkan dengan perkembangan tekonologi informasi adalah masalah keamanan data, maka upaya yang harus dilakukan oleh pemilik dan pengelola sistem informasi yaitu memastikan data yang disimpan aman dari korupsi dan memastikan bahwa akses hanya digunakan oleh yang berwenang, yang bertujuan untuk melindungi data dari ancaman yang disengaja atau tidak disengaja terhadap akses dan integritas. Hal ini menjadi salah satu aspek penting dalam sebuah sistem informasi. Permasalahan keamanan data menjadi perhatian besar bagi pengelola sistem informasi yang di anggap penting dan harus dicari penyelesaian masalahnya. Apapun bentuk informasinya, atau dengan cara apa itu dibagikan atau disimpan, harus selalu tepat terlindung. (ISO & IEC, 2013).

Masalah keamanan data menjadi semakin serius karena tren pencurian data menjadi meningkat (Samuel, 2020). 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. (Kominfo, 2020). Hal ini menyebabkan kerugian tidak hanya materil tetapi juga psikis korban, dimana mereka bisa saja mendapatkan perlakuan diskriminasi di lungkungan masyarakat. Pada tahun 2017, dua rumah sakit di Indonesia terjangkit program jahat jenis ransomware bernama WannaCry yang mengunci data sistem informasi rumah sakit dan meminta tebusan. Jika data

kondisi dan riwayat penyakit berhasil dicuri, potensi kerugian yang dihadapi pemilik data tidak hanya menyangkut persoalan ekonomi tapi dapat menyangkut kerugian sosial budaya hingga keamanan. (Samuel, 2017)

Pelaku pembobolan atau pencurian data kesehatan kesehatan tidak hanya dari pihak luar fasilitas pelayanan kesehatan. Pihak internal juga membobol data, dengan persentase mencapai 39% dari total kasus. Faktor ekonomi menjadi motif utama para pelaku (91%). Hal ini karena banyaknya informasi individu yang ada di dalam sebuah data kesehatan. Bagi fasilitas pelayanan kesehatan, bocornya data pribadi pasien selain membuat kerugian ekonomi juga akan mengganggu jalannya pelayanan serta merusak nama baik dan kepercayaan publik. Bocornya data pribadi seperti tanggal lahir, nomor telepon, alamat, hingga email pribadi dapat digunakan oleh pihak tidak bertanggung jawab untuk melakukan kejahatan. (Irwandy, 2020)

Disebutkan dalam penelitian Ningtyas & Lubis (2018) dijelaskan bahwa 70% orang mengkhawatirkan jika informasi kesehatan mereka terkait data pribadi mengalami kebocoran. Hal ini sudah dibuktikan dengan adanya penjualan data pasien pada Rumah Sakit Universitas Chicago dan Rumah Sakit Wilcox Memorial, Kauai, Hawaii (sebanyak 130.000 data pasien), kejadian tersebut membuktikan bahwa meskipun RME merupakan solusi yang baik untuk penyajian, penyimpanan, dan pengolahan data secara real-time, namun masih memiliki permasalahan yaitu bagaimana data disimpan dan mengalir pada sistem dengan aman dan tetap terjaga kerahasiaannya.

Prinsip Keamanan informasi khususnya dalam bidang kesehatan mencakup enam aspek yaitu *privacy, integrity, authentication, availability, access control* dan *non repudiation*. (Sabarguna, 2008). Berdasarkan penelitiaan Nugraheni (2018) yang dilakukan di RSUD dr. Moewardi diperoleh hasil bahwa di rumah sakit tersebut belum terdapat fasilitas tanda tangan elektronik, hal itu tidak sesuai dengan aspek *authentication.* Berdasarkan aspek *integrity,* rekam medik elektronik pada Rumah Sakit dr.Moewardi juga belum memfasilitasi perubahan informasi dimana pencoretan/penghapusan tidak dapat dilakukan. Hal tersebut dapat meingkatkan resiko ketidakamanan rekam medis dari pihak yang tidak bertanggung jawab.

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.

Berdasarkan latar belakang yang telah dipaparkan, mengingat pentingnya fasilitas kesehatan dalam menjaga keamanan data pribadi pasien dalam pelaksanaan rekam medis elektronik, serta dampak yang ditimbulkan apabila informasi dalam rekam medis pasien bocor dan berisiko akan digunakan oleh pihak yang tidak bertanggungjawab, peneliti tertarik melakukan penelitian dengan judul "Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan Rekam Medik Elektronik Di Fasilitas Kesehatan (*Literature Review*)" untuk mengetahui lebih lanjut bagaimana implementasi rekam medik elektronik di fasilitas kesehatan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, dapat dilakukan perumusan masalah dalam penelitian yang dibuat menggunakan metode PICO, sebagai berikut :

Tabel 1.1 Perumusan Masalah Menggunakan Metode *PICO*

Metode PICO	
Problem	Keamanan data pasien
Intervention	Analisis keamanan informasi data pasien pada penerapan rekam medik elektronik
Comparison	6 aspek keamanan informasi
Outcome	Tingkat keamanan informasi data pasien pada penerapan rekam medik elektronik berdasarkan aspek keamanan informasi

Sehingga rumusan masalah dari penelitian ini adalah “Bagaimana aspek keamanan informasi data pribadi pasien pada rekam medik elektronik di fasilitas kesehatan?”

1.3 Tujuan penelitian

1.3.1 Tujuan Umum

Mengetahui keamanan informasi data priadi pasien pada rekam medik elektronik di fasilitas kesehatan.

1.3.2 Tujuan Khusus

1. Mengetahui penerapan aspek *privacy* pada rekam medik elektronik di fasilitas kesehatan.
2. Mengetahui penerapan aspek *integrity* pada rekam medik elektronik di fasilitas kesehatan.

3. Mengetahui penerapan aspek *authentication* pada rekam medik elektronik di fasilitas kesehatan.
4. Mengetahui penerapan aspek *availability* pada rekam medik elektronik di fasilitas kesehatan.
5. Mengetahui penerapan aspek *acces control* pada rekam medik elektronik di fasilitas kesehatan.
6. Mengetahui penerapan aspek *non-repudiation* pada rekam medik elektronik di fasilitas kesehatan.

1.4 Manfaat Penelitian

1.4.1 Bagi Rumah Sakit

Penelitian ini bermanfaat sebagai bahan evaluasi bagi rumah fasilitas kesehatan terkait aspek keamanan data pasien pada rekam medik elektronik

1.4.2 Bagi Peneliti

1. Penelitian ini bermanfaat sebagai salah satu syarat untuk menyelesaikan pendidikan di program studi Manajemen Informasi Kesehatan jurusan Kesehatan Politeknik Negeri Jember
2. Penelitian ini bermanfaat sebagai proses pembelajaran untuk meningkatkan pengetahuan serta kemampuan berfikir peneliti

1.4.3 Bagi Politeknik Negeri Jember

Penelitian ini bermanfaat sebagai referensi kepustakaan serta arsip yang dapat dimanfaatkan oleh mahasiswa maupun peneliti lain

1.5 Ruang lingkup

Ruang lingkup permasalahan yang akan dibahas dalam penulisan *literature review* ini adalah bagaimana keamanan informasi data pasien pada rekam medik elektronik ditinjau dari 6 aspek keamanan. Aspek *privacy* adalah penjagaan informasi dari pihak yang tidak memiliki hak untuk mengakses informasi. *Integrity* berkaitan dengan perubahan informasi. *Authentication* berkaitan dengan akses terhadap informasi. *Availability* atau ketersediaan adalah aspek yang menekankan pada ketersediaan informasi apabila dibutuhkan oleh pihak terkait. *Access control* berkaitan pada cara pengaturan akses terhadap informasi. *Non repudiation* erat kaitannya dengan suatu transaksi atau perubahan informasi.

1.6 Keaslian Penelitian

Perbedaan dan persamaan penelitian yang dilakukan antara peneliti lain dengan peneliti adalah sebagai berikut:

Table 1.2 *State Of The Art*

Peneliti	Wahyuli vera setiana putri (2017)	Dea Anjani, Apol Pribadi Subriadi, Anisah Hediyanti (2020)	Siti Sofia (2022)
Judul	Tinjauan keamanan data rekam edis pasien pada aplikasi *primary care* di puskesmas bangkalan	Identifikasi, penilaian, dan mitigasi risiko keamanan informasi pada sistem electronic medical record	Analisis aspek keamanan informasi data pribadi pasien pada penerapan rekam medik elektronik
Tujuan	Meninjau keamanan data rekam medis pasien pada aplikasi *primary care* di puskesmas	Mengidentifikasi, menilai dan memitigasi risiko yang berkaitan dengan aplikasi healthty plus yang merupakan Electronic Medical Record (EMR) sistem yang digunakan Rumah Sakit Umum Haji	Menganalisis keamanan informasi data pasien pada penerapan rekam medik elektronik di fasilitas kesehatan
Metode	Kualitatif	Kualitatif	*Literature review*
Ruang Lingkup	Keamanan rekam medik elektronik ditinjau dari aspek *authentication, authorization, integrity, audit trails, disaster and recovery*	Keamanan rekam medik elektronik ditinjau dari FMEA (Failure Modes and Effect Analysis)	keamananan rekam medik elektronik ditinjau dari beberapa aspek aspek keamanan informasi yaitu *privacy* atau *confidentiality, integrity, authentication, availability, access control* dan *non repudiation*.

Hasil	Aspek *authorization* diterapkan dengan pengaksesan menu tertentu sesuai kewenangannya, aspek *audit trails* berupa penanggung jawab dapat memantau aktivitas dan menjalankan sistem tersebut, aspek *disaster recovery* diterapkan jika data rusak maka dapat dipulihkan kembali.	penilaian risiko menggunakan metode FMEA*(Failure Mode & Effect Analysis)* didapatkan risiko yang mempunyai skor assessment tertinggi hingga terendah. Penyalahgunaan hak akses dan untuk risiko palingrendah dengan nilai RPN 18 terdapat pada risiko *Backup data failure*.	aspek *privacy* diterapkan dengan penggunaan *username* dan *password*, aspek *integrity* diterapkan dengan perubahan atau penghapusan data oleh administrator, aspek *authentication* diterapkan dengan adanya tanda tangan elektronik dan penggunaan PIN, Aspek *availability* dibuktikan dengan menggunakan proses *backup* data guna mengantisipasi peretasan data pasien, aspek *acces control* dilakukan pembatasan hak akses dengan penggunaan *user id & password* bagi masing-masing pengguna, Aspek *non repudiation* diterapkan dengan adanya *log file*