

BAB 1. PENDAHULUAN

1.1 Latar Belakang

Saat ini dunia sedang berada pada masa di mana keberadaan informasi mempunyai peranan yang sangat penting dalam kehidupan manusia. Kemajuan informasi, komunikasi, dan teknologi merupakan salah satu faktor utama yang mendorong perkembangan dan pertumbuhan ekonomi dunia. Saat ini informasi merupakan komoditas dengan nilai ekonomi yang tinggi, hal tersebut dikarenakan tidak semua pihak mampu untuk memproses suatu data mentah menjadi suatu informasi yang sesuai dengan kebutuhan.

Teknologi Informasi dan Komunikasi (TIK) memainkan peran penting dalam mendukung kehidupan sehari-hari, tak terkecuali pada bidang kesehatan (Rosadi, 2016). Pemanfaatan Teknologi Informasi dan Komunikasi (TIK) dalam bidang kesehatan salah satunya adalah rekam medis elektronik. Bentuk rekam medis tidak hanya berupa data dokumen/kertas melainkan dapat berupa data elektronik.

Institute of Medicine (1999) menjelaskan bahwa rekam kesehatan berbasis komputer (*Computer-based patient record/CPR*) adalah rekaman pasien yang dikerjakan secara elektronik dan bernaung dalam sistem yang dirancang secara khusus. Kegunaannya mendukung pengguna dalam mengakses data secara lengkap dan akurat, yakni dengan memberikan tanda peringatan, waspada, dan sistem pendukung pengambilan keputusan klinis yang merujuk data kepada sumber pengetahuan medis dan sarana bantuan lainnya. Rekam medis elektronik atau *electronic medical record* bukan merupakan hal yang baru di negara maju seperti Korea, Inggris, dan Jepang. Menurut Kruse (2017) dalam Tiorentap dan Hosizah (2020) rekam medis elektronik merupakan catatan medis yang berbentuk elektronik, dan dikelola oleh penyedia layanan kesehatan yang mana didalamnya berisi data demografi, catatan kemajuan, permasalahan, pengobatan, tanda-tanda vital, riwayat pengobatan sebelumnya, imunisasi, hasil laboratorium, dan laporan radiologi. Menurut Hughes (2008) *electronic medical record* atau rekam medis

elektronik merupakan kumpulan informasi kesehatan elektronik untuk dan tentang pasien, yang digunakan untuk mendukung efisiensi pelayanan.

Rekam medis elektronik atau *electronic medical record* merupakan sebuah proses dan proyek besar yang penuh dengan tantangan (Dwijosusilo & Sarni, 2018). Seluruh kemudahan dan manfaat yang dihasilkan dari penerapan rekam medis elektronik tidak terlepas dari ancaman yang harus diantisipasi. Data kesehatan rawan sekali mengalami kebocoran, hal tersebut dikarenakan *mindset* bahwa data tidak berkaitan dengan uang (Tiorentap dan Hosizah, 2020). Menurut Direktorat Proteksi Infrastruktur Informasi Kritis Nasional (IIGN) Badan Siber dan Sandi Negara (2019) keamanan data dari sektor kesehatan harus diprioritaskan, mengingat teknik dan kasus pencurian data saat ini telah bervariasi, meliputi penyanderaan data oleh *ransomware*, risiko dari pihak ketiga, dan kerawanan *email* serta *mobile application*.

Kasus mengenai keamanan data yang sempat ramai terjadi pada Februari 2017. Beberapa rumah sakit di Jakarta mengalami serangan *ransomware Wannacry*. Pada kasus tersebut, *hacker* meminta tebusan sebesar Rp4.000.000,- yang harus dibayarkan dalam bentuk Bitcoin. Kasus tersebut dinyatakan sebagai salah satu serangan *cyber* terbesar yang pernah terjadi di dunia. *Ransomware* menyebabkan terjadinya kelumpuhan sistem. Sehingga sistem tidak dapat menarik nomor antrian dikarenakan piranti lunak terkunci dan data pasien terenkripsi. Hal tersebut menimbulkan kelambatan sistem yang berakibat pada penumpukan pasien.

Berdasarkan ketentuan dari *Health Insurance Portability and Accountability Act (HIPAA)* keamanan sistem informasi kesehatan harus memenuhi beberapa aspek, antara lain : a) kerahasiaan, integritas, dan ketersediaan semua informasi kesehatan yang dilindungi dalam membuat, menerima, mempertahankan, atau mentransmisikan informasi kesehatan. b) melindungi terhadap ancaman atau bahaya yang diantisipasi secara wajar. c) melindungi dari penggunaan atau pengungkapan informasi yang diantisipasi secara wajar berdasarkan peraturan privasi. d) pastikan kepatuhan oleh tenaga kerjanya.

Menurut Rahardjo (2005) prinsip keamanan informasi dapat mencakup *privacy*, *confidentiality*, *integrity*, *availability*, *non repudiation*, *authentication*, dan *authorization*. Pendapat ini sejalan dengan aturan dari *ISO/IEC 27001* yang menjelaskan bahwa aspek keamanan informasi mencakup *confidentiality*, *integrity*, dan *privacy*. Menurut Sabarguna (2008) dalam Nugraheni dan Nurhayati (2018) hal utama dari aspek *privacy* atau *confidentiality* adalah penjagaan informasi dari pihak-pihak yang tidak memiliki hak untuk mengakses informasi. *Integrity* berkaitan dengan perubahan informasi. *Authentication* berhubungan dengan akses terhadap informasi. *Availability* atau ketersediaan adalah aspek yang menekankan pada ketersediaan informasi apabila dibutuhkan oleh pihak-pihak terkait. *Access control* adalah aspek yang menekankan pada cara pengaturan akses terhadap informasi. *Non repudiation* erat kaitannya dengan suatu transaksi atau perubahan informasi.

Berdasarkan hasil wawancara dan observasi mengenai penerapan *Electronic Medical Record* atau rekam medis elektronik di Rumah Sakit PHC Surabaya, ditemukan beberapa permasalahan prinsip keamanan sistem informasi. Fitur logout otomatis hanya diterapkan dalam ERM Rawat Jalan khusus dokter saja, sedangkan ERM Rawat Jalan khusus petugas rekam medis dan ERM Rawat inap belum dilengkapi fitur tersebut. Sedangkan pada ruangan rekam medis banyak sekali pihak selain petugas rekam medis yang bebas keluar masuk ke ruangan. Selain itu, petugas rekam medis juga seringkali tidak mematikan PC dan melogout aplikasi ERM saat ditinggalkan dan tidak digunakan. Hal ini memungkinkan sistem dapat dikases oleh pengguna yang tidak berhak dan kebocoran informasi dapat terjadi. Selain itu berdasarkan hasil wawancara dengan petugas rekam medis dan petugas IT, didapatkan informasi bahwa belum pernah dilakukan audit sistem informasi rekam medis elektronik. Audit sistem informasi adalah proses pengumpulan dan penilaian bukti-bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumber daya secara efisien (Cantika, 2020).

Berdasarkan latar belakang yang telah dipaparkan, peneliti tertarik untuk mengetahui aspek keamanan informasi dalam penerapan rekam medis elektronik di Rumah Sakit PHC Surabaya, dengan melakukan mini riset yang berjudul “Analisis Aspek Keamanan Informasi Pasien dalam Penerapan Rekam Medis Elektronik di Rumah Sakit PHC Surabaya”.

1.2 Tujuan dan Manfaat

1.2.1 Tujuan Umum PKL

Mengetahui aspek keamanan informasi pasien dalam penerapan rekam medis elektronik di Rumah Sakit PHC Surabaya.

1.2.2 Tujuan Khusus PKL

1. Menganalisis aspek keamanan informasi dalam penerapan rekam medis elektronik di Rumah Sakit PHC Surabaya berdasarkan aspek kerahasiaan (*confidentiality*)
2. Menganalisis aspek keamanan informasi dalam penerapan rekam medis elektronik di Rumah Sakit PHC Surabaya berdasarkan aspek integritas (*integrity*)
3. Menganalisis aspek keamanan informasi dalam penerapan rekam medis elektronik di Rumah Sakit PHC Surabaya berdasarkan aspek autentikasi (*authentication*)
4. Menganalisis aspek keamanan informasi dalam penerapan rekam medis elektronik di Rumah Sakit PHC Surabaya berdasarkan aspek ketersediaan (*availability*)
5. Menganalisis aspek keamanan informasi dalam penerapan rekam medis elektronik di Rumah Sakit PHC Surabaya berdasarkan aspek kontrol akses (*access control*)
6. Menganalisis aspek keamanan informasi dalam penerapan rekam medis elektronik di Rumah Sakit PHC Surabaya berdasarkan aspek nir-sangkal (*non repudiation*)

1.2.3 Manfaat PKL

1. Memperluas materi pembelajaran mengenai manajemen informasi kesehatan serta sebagai referensi dalam pengembangan penelitian yang lebih lanjut

2. Mempelajari kondisi di lapangan serta menambah pengalaman di instansi kesehatan, khususnya mengenai pelaksanaan manajemen informasi kesehatan
3. Mengetahui dan menganalisis permasalahan terkait keamanan rekam medis elektronik serta menghasilkan rekomendasi yang berguna untuk pengembangan rekam medis elektronik

1.3 Lokasi dan Waktu

Penelitian dilaksanakan saat Praktek Kerja Lapang (PKL) di Rumah Sakit Primasatya Husada Citra (PHC) Surabaya. Penelitian dilakukan selama 3 bulan, mulai 3 Januari – 12 April 2022.

1.4 Metode Pelaksanaan

1.4.1 Subjek dan Objek Penelitian

Subjek penelitian adalah Profesional Pemberi Asuhan (PPA), petugas rekam medis, dan petugas IT. Objek penelitian adalah rekam medis elektronik di Rumah Sakit PHC Surabaya.

1.4.2 Instrumen Pengumpulan Data

1. Kuesioner Google Form

Kuesioner berisi pertanyaan terbuka dan tertutup mengenai penerapan rekam medis elektronik.

2. Pedoman Wawancara

Pedoman wawancara berupa daftar pertanyaan yang sudah disusun dan digunakan untuk memperkuat pedoman observasi guna mendapatkan informasi mengenai fitur keamanan data pada sistem rekam medis elektronik.

3. Pedoman Observasi

Daftar pedoman pengamatan yang dibentuk dalam analisis keamanan data pasien dalam penerapan rekam medis elektronik.

1.4.3 Cara Pengumpulan Data

1. Menyebar Kuesioner

Kuesioner disebar kepada masing-masing Profesional Pemberi Asuhan (PPA) dan petugas rekam medis.

2. Wawancara

Wawancara adalah suatu proses tanya jawab yang dilakukan dengan cara bertatap muka langsung dengan responden. Wawancara dilakukan dengan petugas IT untuk mengetahui lebih dalam mengenai fitur keamanan yang ada pada ERM Rumah Sakit PHC Surabaya serta dengan petugas rekam medis selaku pembuat kebijakan atau *Business Process Owner*.

3. Observasi

Observasi adalah suatu proses pengumpulan data yang dilakukan dengan cara mengamati proses penggunaan secara langsung. Observasi dilakukan dengan cara mengamati secara langsung proses penggunaan rekam medis elektronik di Rumah Sakit PHC Surabaya serta mempelajari Standar Prosedur Operasional (SPO).

1.4.4 Teknik Pengolahan Data

1. *Collecting*

Pengumpulan data aspek-aspek keamanan dari hasil menyebar kuesioner, wawancara, dan observasi. Aspek-aspek keamanan antara lain *confidentiality*, *integrity*, *authentication*, *availability*, *access control*, dan *non repudiation*.

2. Klasifikasi

Mengelompokkan dan memilah data sesuai dengan kelompok data aspek keamanan.

3. *Editing*

Mengoreksi dan memperbaiki data yang telah diperoleh menjadi informasi yang terbaru.

4. Penyajian Data

Disajikan dengan menggambarkan hasil penelitian.

1.4.5 Analisis Data

Analisis data yang digunakan adalah secara deskriptif dengan memaparkan hasil penelitian sesuai dengan keadaan sebenarnya mengenai aspek keamanan data pasien dalam penerapan rekam medis elektronik di Rumah Sakit PHC Surabaya.

1.5 Kerangka Konsep

