BAB 1. PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi dan komunikasi yang selanjutnya di singkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, pengelolaan dan penyampaian atau pemindahan informasi antar sarana atau media (Kominfo, 2012). Kebutuhaan untuk menggunakan teknologi informasi saat ini diperlukan untuk mendukung kinerja sebuah organisasi, teknologi informasi telah menjadi kebutuhan bagi semua bidang salah satunya adalah dalam layanan kesehatan. Dengan penggunaan sistem informasi dalam layanan kesehatan dapat memberikan banyak manfaat yang sangat menguntungkan bagi penyedia layanan kesehatan, seperti meningkatkan kualitas pelayanan, mengurangi kesalahan medis, meningkatkan pembacaan ketersediaan fasilitas dan aksesibilitas infromasi (Tiorentap&Hosizah, 2020)

Rumah sakit merupakan salah satu instistusi pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan perorangan secara paripurna baik rawat inap, rawat jalan, dan gawat darurat tentunya berkewajiban untuk menyelenggarakan rekam medis elektronik yang dilakukan sejak pasien masuk sampai pasien pulang, Rekam medis elektronik adalah dokumen yang berisikan data identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang telah diberikan kepada pasien. dirujuk, atau meninggal. (Kemenkes RI, 2022). Menurut *Institute Of Medicine (1999)* rekam kesehatan berbasis komputer (*Comupter-based patient record/*CPR) merupakan rekaman pasien yang dikerjakan secara elektronik dan berada di dalam sistem yang dirancang secara khusus untuk mendukung pengguna dalam mengakses data pasien secara lengkap dan akurat, yaitu dengan memberikan tanda peringatan, waspada, dan sistem pendukung pengambil keputusan klinis (Ramadhanti, 2022).

Terlepas dari berbagai manfaat yang dapat dirasakan dari penggunaan sistem rekam medis elektronik dalam bidang kesehatan, tentunya terdapat beberapa ancaman yang harus menjadi perhatian khusus bagi instnasi penyedia pelayanan kesehatan. Dengan pesatnya penggunaan teknologi informasi saat ini, dibutuhkan

tata kelola teknologi informasi untuk menjaga keamanan informasi dan data (Musyarofah&Bisma, 2020). Tren pencurian data yang terus meningkat menjadi permasalahan yang serius. Pencurian data kesehatan bukan hal baru di Indonesia. Pada tahun 2020 sebanyak 230 data pasien Covid-19 diketahui telah dicuri data kesehatannya, selain itu pada bulan januari tahun 2022 diduga telah terjadi pelanggaran data pada catatan pasien di beberapa rumah sakit di Indonesia sebesar 720 GB yang dijual di forum online (Sofia et al., 2022). *Ransomeware WannaCry* merupakan kasus kebocoran data terbesar didunia dimana dalam kasus ini sebanyak 150 negara menjadi korban dan mengakibatkan kelumpuhan sistem salah satunya adalah sistem informasi di Rumah Sakit Kanker Dharmais yang mengalami kelumpuhan sistem akibat dari hal tersebut dan menyebabkan penumpukan pasien (Tiorentap&Hosizah, 2020).

Permenkes RI no 24 tahun 2022 tentang rekam medis telah mengatur tekait dengan keamanan rekam medis elektronik dimana rekam medis diselenggarakan secara elektronik dengan tujuan menjamin kemanan, kerahasiaan, keutuhan, dan ketersediaan data rekam medis yanag harus memenuhi prinsip-prinsip keamanan data dan informasi yaitu kerahasiaan, integritas dan ketersediaan data (Kemenkes RI, 2022). Menurut *Health Insurance Portability and Acountability Act (HIPAA)* keamanan informasi haru memenuhi beberapa hal yaitu, 1) Memastikan kerahasiaan, integritas, dan ketersediaan semua informasi kesehatan serta melindungi dalam membuat, menerima, mempertahankan, atau mentransmisikan informasi kesehatan; 2) Melindungi dari ancaman dan bahaya yang diantisipasi secara wajar; 3) Melindungi dari pengguna atau penggungkapan informasi yang diantisipasi secara wajar berdasarkan perturan privasi; 4) Memastikan kepatuhan tenaga kerja (Tiorentap&Hosizah, 2020).

Standar ISO/IEC 27001:2013 yaitu acuan standar sistem manajemen keamanan informasi yang dikeluarkan oleh "*International Organization for Standarization dan International Comission*" yang terdiri dari aspek keamanan informasi *confidently* (kerahasiaan), *availability* (ketersediaan), dan *integrity* (integritas). ISO/IEC 27001:2013 memberikan kerangka pembangunan, penerapan,

pengoperasian, pemantauan, peminjaman dan peningkatan Sistem Manajemen Keamanan Informasi (SMKI) (Musyarofah&Bisma, 2020). Rahardjo (2005) menjelaskan bahwa prinsip keamanan mencakup *privacy*, *confidently*, *integrity*, *avaibility*, *nonrepudiation*,*authentication* dan *authorization*. Menururt Sabarguna (2008) dalam Nugraheni dan Nurhayati (2018) aspek *privacy* atau *confidentiality* merupakan penjagaan informasi dari pihak-pihak yang tidak memiliki hak untuk mengakses informasi. *Integrity* merupakan bagaimana tentang perubahan informasi. *Authentication* berkaitan dengan bagaimana akses terhadap informasi. *Availability* merupakan ketersediaan informasi bila dibutuhkan oleh pihak-pihak terkait. *Acces Contro*l merupakan cara pengaturan akses informasi dan Non repudiation merupakan transaksi informasi atau perubahan informasi.

Berdasarkan hasil wawancara dan observasi terkait rekam medis elektronik di Rumah Sakit Bethesda Yogyakarta, diketahui terdapat beberapa permasalahan terkait keamanan rekam medis elektronik. Rekam medis elektronik akan terlog out secara otomatis apabila E-RM sudah tidak digunakan selama kurang lebih dari enam jam. Beberapa petugas tidak mematikan PC dan melogout rekam medis elektronik Ketika ditinggalkan dan tidak digunakan. Diketahui beberapa petugas belum melakukan penggantian *username* dan *password* secara berkala, hal ini penting dilakukan untuk menjaga kerahasiaan E-RM, apabila *username* dan *password* tersebut telah diketahui oleh pihak yang tidak berkepentingan. Kontrol akses dalam rekam medis elektronik dapat di implementasian melalui penggunaan *username* dan *password.* Selain itu diketahui belum adanya standar operasional prosedur (SOP) terakit penyelenggaran rekam medis elektronik atau SOP khusus terkait keamanan dan kerahasiaan data pasien dalam rekam medis elektornik. Standar operasional prosedure (SOP) mampu mengurangi dan menghindari kerentanan ancaman kemanan informasi serta menjadi pedoman dalam menjalankan aktivitas yang berkaitan dengan keamanan informasi (Musyarofah&Bisma, 2020).

Berdasarkan permasalahan yang telah dijelaskan dalam latar belakang serta mengingat pentingnya menjaga keamanan data pasien, peneliti tertarik untuk

meneliti terkait aspek keamanan rekam medis eletronik di Rumah sakit Betehsda Yogyakarta dengan judul "Analisis Aspek Keamanan Data Pasien Dalam penerapan Rekam Medis Elektronik di Rumah Sakit Bethesda Yogyakarta".

1.2 Tujan dan Manfaat

1.2.1 Tujuan Umum MAGANG/PKL

Mengetahui aspek keamanan informasi pasien dalam penerapan rekam medis elektronik di Rumah Sakit Bethesda Yogyakarta.

1.2.2 Tujuan Khusus MAGANG/PKL

1. Menganalisis aspek keamanan data pasien dalam penerapan rekam medis elektronik di Rumah Sakit Bethesda Yogyakarta berdasarkan aspek kerahasiaan (*confidentiality*).
2. Menganalisis aspek keamanan data pasien dalam penerapan rekam medis elektornik di Rumah Sakit Bethesda Yogyakarta berdasarkan aspek integritas (*integrity*).
3. Menganalisis aspek keamanan data pasien dalam penerapan rekam medis elektronik di Rumah Sakit di Rumah Sakit Bethesda Yogyakarta berdasarkan aspek autentikasi (*authentication*).
4. Menganalisis aspek keamanan data pasien dalam penerapan rekam medis elektronik di Rumah Sakit Bethesda Yogyakarta berdasarkan aspek ketersediaan (*availability*).
5. Menganalisis aspek keamanan data pasien dalam penerapan rekam medis elektronik di Rumah Sakit Bethesda Yogyakarta berdasarkan aspek akses kontrol (*access control*).
6. Mengalisis aspek keamanan data pasien dalam penerapan rekam medis elektronik di Rumah Sakit Bethesda Yogyakarta berdasarkan aspek nir-sangkal (*nonrepudiation*).

1.2.3 Manfaat MAGANG/PKL

1. Bagi Rumah Sakit

Diharapakan penelitian yang telah dilakukan dapat dijadikan bahan refrensi atau pertimbangan dalam proses evaluasi rekam medis elektronik terutama dalam aspek keamanan data pasien.

2. Bagi Politeknik Negeri Jember

   Diharpkan penelitian yang telah dilakukan dapat menjadi bahan refrensi bagi penelitian selanjutnya, serta pembelajaran dan pengembangan ilmu pengetahuan bagi mahasiswa Politeknik Negeri Jember khususnya bagi mahasiswa Manajemen Informasi Kesehatan.

3. Bagi Mahasiswa

   Mahasiswa mampu menerapkan ilmu pengetahuan yang telah didapat selama di bangku perkuliahan dan selama praktek kerja lapang di Rumah Sakit Bethesda Yogyakarta, serta menambah pengetahuan mahasiswa terkait keamanan data pasien dalam pelaksanaan rekam emdis elektronik di Rumah Sakit Bethesda Yogyakarta.

1.3 Lokasi dan Waktu

Penelitian dilakukan di Rumah Sakit Bethesda Yogyakarta yang beralamtkan di Jl. Jendral Sudirman 70, Kotabaru, Kec.Gondokusuman, Kota Yogakrta Daerah Istimewa Yogyakarta. Yang dilaksanakan selama 3 bulam mulai dari tanggal 2 Oktober – 23 Desember 2023.

1.4 Metode Pelaksanaan

1.4.1 Sumber Data

a. Data Primer

   Menururt Bungin, data primer adalah data yang langsung diperoleh dari sumber data pertama di lokasi penelitian atau objek penelitian (Rahmadi, 2011). Data primer dalam penelitian ini diperoleh dari hasil wawancara dan observasi langsung dengan informan terkait dengan aspek keamanan data pasien dalam rekam medis elektronik di Rumah Sakit Bethesda Yogyakarta.

b. Data Sekunder

Menurut Bungin, data sekunder adalah data yang diperoleh dari sumber kedua atau tidak langsung dari data yang dibutuhkan (Rahmadi, 2011). Data sekunder dalam penelitian ini diperoleh dari pengumpulan data infromasi melalui dokumen, jurnal, buku, atau skripsi yang sesuai dengan topik penelitian yang dapat mendukung data primer.

1.4.2 Teknik pengumpulan Data

a. Observasi

Dalam penelitian ini observasi dilakukan dengan cara pengamatan dan pemantauan petugas serta sarana dan prasarana terkait dengan aspek keamanan data pasien dalam rekam medis elektronik.

b. Wawancara Mendalam

Wawancara mendalam merupakan pengumpulan informasi secara langsung dengan informan dengan cara tanya jawab secara mendalam untuk memperoleh keterangan serta penjelasan terkait *privacy, confidently, integrity, avaibility, nonrepudiation,authentication* dan *authorization* yang berkaitan dengan aspek keamanan data pasien dalam rekam medis elektronik di Rumah sakit Bethesda Yogyakarta.

c. Dokumentasi

Pengumpulan data dalam dokumentasi dilakukan dengan maksud untuk memberikan bukti yang akurat terkait dengan kebenaran data. Adapun dokumentasi yang dilakukan berupa hasil foto, rekaman, dokumen atau berkas, peraturan-peraturan atau data yang sesuai dengan penelitian yang diperoleh saat melakukan penelitian di Rumah sakit Bethesda Yogyakarta.