BAB 1. PENDAHULUAN

1.1 Latar Belakang

Rumah sakit adalah institusi pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan perorangan secara paripurna yang menyediakan pelayanan rawat inap, rawat jalan, dan gawat darurat. Pelayanan kesehatan paripurna merupakan pelayanan kesehatan yang mencakup tindakan promotif, preventif, kuratif, serta rehabilitatif. Suatu pelayanan kesehatan akan berjalan dengan baik apabila didukung dengan pelayanan yang baik pula, sehingga mampu memberikan pelayanan yang bermutu salah satunya dengan pelayanan rekam medis (Kementerian Kesehatan RI, 2009).

Rekam medis merupakan berkas yang berisikan catatan dan dokumen mengenai identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang telah diberikan kepada pasien. Isi rekam medis harus dijaga kerahasiaannya oleh seluruh pihak yang terlibat dalam pelayanan kesehatan pada fasilitas pelayanan kesehatan. Perkembangan teknologi digital di masyarakat menyebabkan adanya transformasi digitalisasi pelayanan kesehatan, sehingga rekam medis perlu diselenggarakan secara elektronik dengan prinsip keamanan, kerahasiaan data dan informasi. Mengacu pada peraturan terbaru Kementerian Kesehatan Republik Indonesia yang menyatakan bahwa seluruh fasilitas pelayanan kesehatan wajib untuk menyelenggarakan rekam medis elektronik paling lambat 31 Desember 2023 (Kementerian Kesehatan RI, 2022).

Rekam medis elektronik adalah rekam medis yang dibuat dengan menggunakan sistem elektronik (Kementerian Kesehatan RI, 2022). Rekam medis elektronik diselenggarakan untuk mencapai penyelenggaraan pelayanan kesehatan yang cepat, akurat, efisien, dan kemudahan pelaporan. Segala kemudahan dan manfaat dari implementasi rekam medis elektronik tidak lepas dari ancaman yang wajib diantisipasi oleh setiap fasilitas pelayanan kesehatan. Salah satu permasalahan utama terkait perkembangan teknologi informasi yaitu masalah keamanan data (Handiwidjojo, 2009).

Keamanan data adalah perlindungan data dalam suatu sistem untuk menghindari pengguna yang tidak berhak dan modifikasi terhadap data yang telah tersimpan (Herdianto et al., 2021). Upaya yang harus dilaksanakan oleh pemilik dan pengelola sistem informasi yakni memastikan data yang tersimpan aman dan hak akses hanya digunakan oleh orang yang berwenang, hal tersebut bertujuan untuk melindungi data dari ancaman yang disengaja atau tidak disengaja terhadap akses dan integritas. Saat ini masalah keamanan data menjadi semakin serius karena tren pencurian data semakin meningkat (Irwendy, 2021). Data kesehatan merupakan salah satu data yang rawan mengalami kebocoran dan fatal apabila data yang berhasil bocor adalah rekam medis yang sangat rahasia (Ravlindo & Gunadi, 2022).

Di Indonesia, kasus pencurian data kesehatan bukanlah hal yang baru. Pada tahun 2020, 230 ribu data pasien COVID-19 di Indonesia diduga telah dicuri dan dijual pada RaidForums. Data tersebut berisikan nama, umur, nomor telepon, alamat rumah, Nomor Identitas Kependudukan (NIK), hasil *rapid test*, hasil *Polymerase Chain Reaction* (PCR), hingga status terkait COVID-19 (Hendriyanto, 2021). Dilansir dari detiknews.com, pada tahun 2021, terdapat 279 juta data pasien BPJS Kesehatan bocor dan dijual pada RaidForums. Data pribadi yang bocor meliputi Nomor Identitas Kependudukan (NIK), nama, alamat, nomor telepon, hingga besaran gaji. Dilansir dari cnnindonesia.com pada bulan Januari 2022, terdapat kasus kebocoran 6 juta data medis pasien Covid-19 yang dikelola oleh Kementerian Kesehatan. Data yang bocor merupakan rekam medis pasien yang berukuran 720 GB, data tersebut mencakup identitas detail pasien, alamat rumah, tanggal lahir, Nomor Identitas Kependudukan (NIK), anamnesis, data keluhan utama pasien, diagnosis dengan kode ICD-10, pemeriksaan klinis, ID rujukan, pemeriksaan penunjang, hingga rencana keperawatan. Pada tahun yang sama 2022 dilansir dari cnnindonesia.com juga terjadi kebocoran data PeduliLindungi sebanyak 3.2 miliar data. Data tersebut berupa data vaksinasi, data *history check-in*, dan data kontak *tracing history* data pengguna aplikasi PeduliLindungi. Kebocoran data pribadi seperti tanggal lahir, nomor telepon, alamat, dan *e-mail* pribadi dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk

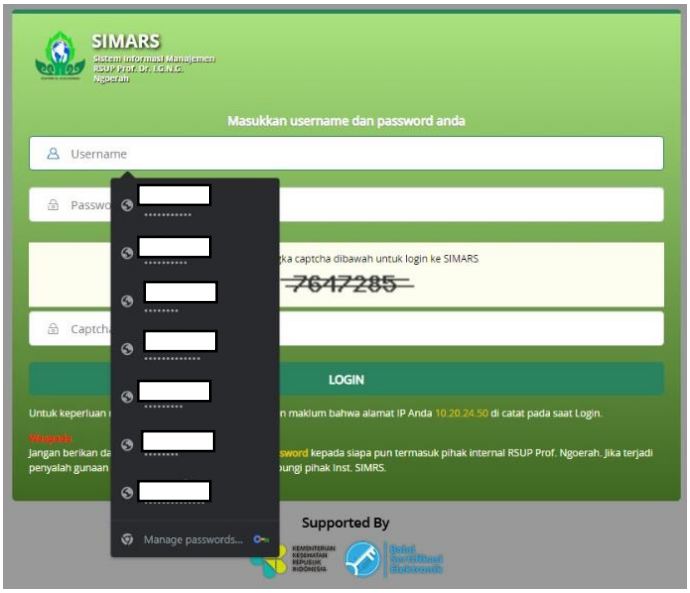
melakukan kejahatan . Dampak kebocoran data kesehatan menjadikan masyarakat merasa tidak aman saat menyimpan informasi data pada lembaga pemerintah ataupun swasta karena beresiko menjadi korban kejahatan *cybercrime* (Anwar et al., 2021).

Berdasarkan kasus terjadinya kebocoran data, rumah sakit yang menyelenggarakan rekam medis elektronik wajib memenuhi prinsip keamanan data dan informasi yaitu kerahasiaan, integritas, dan ketersediaan (Kementerian Kesehatan RI, 2022). Menurut Rahardjo (2017) *dalam* Tiorentap & Hosizah (2020) prinsip keamanan informasi khususnya dalam bidang kesehatan mencakup enam aspek yaitu *privacy* atau *confidentiality*, *integrity*, *authentication*, *availability*, *access control*, dan *non repudiation*. *Privacy* atau *confidentiality* adalah penjagaan informasi dari pihak yang tidak mempunyai hak untuk mengakses informasi. *Integrity* berkaitan dengan perubahan informasi. *Authentication* berhubungan dengan akses terhadap informasi. *Availability* adalah aspek yang menekankan pada tersedianya informasi ketika dibutuhkan oleh pihak yang terkait. *Access control* adalah aspek yang menekankan pada cara pengaturan akses terhadap informasi. *Non repudiation* yaitu berkaitan dengan suatu transaksi atau perubahan informasi (Nugraheni & Nurhayati, 2018).

RSUP Prof. dr. I.G.N.G. Ngoerah merupakan rumah sakit milik pemerintah yang terletak di Denpasar, Bali. RSUP Prof. dr. I.G.N.G. Ngoerah adalah rumah sakit tipe A dan sebagai rumah sakit pusat rujukan untuk Bali, NTB, NTT, dan Timor Timur. Semua pelayanan di RSUP Prof. D dr. I.G.N.G. Ngoerah didukung oleh tenaga kesehatan yang terampil dan profesional, serta dilengkapi dengan peralatan kesehatan yang berteknologi canggih dan mutakhir. RSUP Prof. dr. I.G.N.G. Ngoerah mulai menerapkan SIMARS (Sistem Informasi Manajemen RSUP Prof. dr. I.G.N.G. Ngoerah) sejak tahun 2016, sebagai salah satu penerapan rekam medis elektronik serta untuk menunjang proses pelayanan. Menjadi Rumah Sakit yang telah mengimplementasikan rekam medis elektronik, RSUP Prof. dr. I.G.N.G. Ngoerah perlu memperhatikan kemungkinan adanya ancaman terhadap keamanan dan kerahasiaan data pasien.

Hasil pengamatan peneliti selama melakukan kegiatan PKL ditemukan beberapa permasalahan prinsip keamanan sistem informasi dalam penerapan rekam medis elektronik di RSUP Prof. dr. I.G.N.G. Ngoerah. Selama observasi penggunaan rekam medis elektronik pada SIMARS belum terjamin kerahasiaannya karena bisa diakses selain Profesional Pemberi Asuhan (PPA). Selain itu, petugas seringkali tidak mematikan komputer dan me-*logout* aplikasi saat tidak digunakan. Hal ini memungkinkan terjadi kebocoran informasi akibat dari penyalahgunaan akun untuk mengakses sistem.

Terdapat permasalahan keamanan data rekam medis elektronik yakni pada menu E-MR dapat di *input* atau di edit oleh petugas selain Profesional Pemberi Asuhan (PPA), *password* dan *username* petugas tersimpan di komputer, *password* dan *username* petugas tercatat pada *sticky note*s komputer. Selain itu juga petugas dapat mengerjakan *coding* pasien rawat jalan di luar rumah sakit, hal itu tidak sejalan dengan Modul Kepemilikan Rekam Medis (2022) bahwa tidak dibenarkan membawa rekam medis keluar dari instansi pelayanan kesehatan, kecuali atas izin pimpinan serta dengan sepengetahuan kepala unit rekam medis yang peraturannya telah ditetapkan oleh rumah sakit. Berikut gambar 1.1 merupakan tampilan *username* dan *password* yang tersimpan pada SIMARS.



Gambar 1. 1 Tampilan Username dan Password yang tersimpan pada SIMARS

Berdasarkan latar belakang yang telah diuraikan, mengingat pentingnya RSUP Prof. dr. I.G.N.G. Ngoerah dalam menjaga keamanan data pribadi pasien dalam pelaksanaan rekam medis elektronik, serta dampak yang ditimbulkan apabila informasi dalam rekam medis pasien bocor dan beresiko akan digunakan oleh pihak yang tidak bertanggung jawab, peneliti tertarik untuk melakukan penelitian dengan judul "Analisis Aspek Keamanan Informasi pada SIMARS di RSUP Prof. dr. I.G.N.G Ngoerah Denpasar".

1.2 Tujuan dan Manfaat

1.2.1 Tujuan Umum PKL

Menganalisis aspek keamanan informasi pada SIMARS di RSUP Prof. dr. I.G.N.G Ngoerah Denpasar.

1.2.2 Tujuan Khusus PKL

a. Menganalisis aspek keamanan informasi berdasarkan aspek kerahasiaan (*confidentiality*), integritas (*integrity*), autentikasi (*authentication*), ketersediaan (*availability*), kontrol akses (*access control*), nirsangkal (*non repudiation*) dan Tahap FOCUS (*Focus, Organize, Clarify, Understand, Select*) pada SIMARS di RSUP Prof. dr. I.G.N.G Ngoerah Denpasar.
b. Menganalisis aspek keamanan informasi pada SIMARS menggunakan Tahap PDCA (*Plan, Do, Check, Action*) di RSUP Prof. dr. I.G.N.G Ngoerah Denpasar.

1.2.3 Manfaat PKL

a. Bagi Rumah Sakit

   Penelitian diharapkan dapat menjadi bahan referensi dan pertimbangan dalam proses evaluasi sistem rekam medis elektronik adalah aspek keamanan data pasien.

b. Bagi Politeknik Negeri Jember

   Penelitian ini diharapkan dapat menjadi bahan referensi dan bahan pembelajaran untuk penelitian selanjutnya dalam pengembangan ilmu pengetahuan di Politeknik Negeri Jember.

c. Bagi Mahasiswa

Mahasiswa dapat menerapkan ilmu pengetahuan yang didapat selama kuliah dan selama praktek kerja lapang di RSUP Prof. dr. I.G.N.G Ngoerah Denpasar, serta menambah pengetahuan mahasiswa terkait aspek keamanan informasi pelaksanaan rekam medis elektronik di RSUP Prof. dr. I.G.N.G Ngoerah Denpasar.

1.3 Lokasi dan Waktu

1.3.1. Lokasi

Lokasi Praktek Kerja Lapang (PKL) dilaksanakan di Rumah Sakit Umum Pusat Prof. dr. I.G.N.G Ngoerah.

1.3.2. Waktu

Pelaksanaan waktu Praktek Kerja Lapang yakni pada tanggal 18 September sampai dengan 11 Desember 2023.

1.4 Metode Pelaksanaan

1.4.1 Sumber Data

a. Data Primer

Data primer adalah data yang didapat secara langsung oleh peneliti (Sugiyono, 2013). Data primer dalam penelitian ini didapat dari hasil observasi dan wawancara secara langsung kepada informan yaitu petugas rekam medis dan petugas IT RSUP Prof. dr. I.G.N.G. Ngoerah.

b. Data Sekunder

Data sekunder adalah data yang didapat secara tidak langsung yang melalui hasil pengumpulan data orang lain atau dokumen (Sugiyono, 2013). Data sekunder dalam penelitian ini yaitu jurnal, peraturan, buku, skripsi yang sesuai dengan topik.

1.4.2 Teknik Pengumpulan Data

a. Observasi

Observasi dilakukan langsung oleh peneliti terhadap suatu objek atau subjek yang bertujuan untuk dapat mengamati dan membandingkan kegiatan, perilaku, pengetahuan, serta gagasan yang telah diketahui sebelumnya.

b. Wawancara Mendalam

Peneliti mengumpulkan data dengan menggunakan wawancara mendalam pada variabel *privacy* atau *confidentiality*, *integrity*, *authentication*, *availability*, *access control*, dan *non repudiation* untuk menggali informasi sebanyak-banyaknya guna memperoleh informasi yang relevan dengan aspek keamanan informasi di RSUP Prof. dr. I.G.N.G Ngoerah Denpasar. Proses wawancara mendalam direkam menggunakan rekam suara pada *smartphone* dan dicatat oleh peneliti. Wawancara mendalam kepada informan dapat diakhiri apabila informasi yang diperlukan telah diperoleh sesuai dengan tujuan penelitian. Wawancara mendalam dilakukan guna mengetahui aspek keamanan data SIMARS dalam penerapan rekam medis elektronik Prof. dr. I.G.N.G. Ngoerah Denpasar.

c. Dokumentasi

Dokumentasi adalah cara yang digunakan oleh peneliti untuk menyediakan dokumen dengan adanya bukti yang akurat guna mengetahui kebenaran data. Dokumentasi yang dilakukan oleh peneliti yakni berupa foto, hasil rekaman wawancara, serta peraturan atau data yang berkaitan dengan penelitian yang diperoleh selama melakukan kegiatan penelitian di Prof. dr. I.G.N.G. Ngoerah Denpasar.