BAB 1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dan sistem informasi pada bidang kesehatan sudah mengalami perkembangan yang cukup pesat. Penerapan teknologi informasi di bidang kesehatan dianggap mampu untuk memberikan berbagai utilitas terhadap pelayanan kesehatan seperti tersedianya informasi kesehatan pasien secara tepat dan komprehensif, sehingga diharapkan mampu membantu petugas medis dalam penegakan diagnosa serta meminimalisir terjadinya *medical error* (Cholik, 2021). Salah satu faktor penyebab terjadinya *medical error* adalah pencatatan dan pendokumentasian medis pasien yang tidak efektif (Chegini *et al.*, 2020). Sehingga, teknologi dan sistem informasi dianggap sangat penting bagi perusahaan atau organisasi, salah satunya adalah rumah sakit.

Rumah sakit adalah institusi pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan perorangan secara paripurna dengan menyediakan pelayanan rawat inap, rawat jalan, dan gawat darurat (Kemenkes, 2018). Sehingga sesuai dengan Undang-undang No 44 Tahun 2009, rumah sakit berkewajiban untuk menyelenggarakan pelayanan pengobatan dan pemulihan kesehatan sesuai dengan standar pelayanan rumah sakit. Selain itu, rumah sakit juga diharapkan mampu memberikan pelayanan berkualitas yang secara umum dapat ditinjau dari keberadaan rekam medis sebagai pendokumentasian riwayat medis pasien (Giyana, 2012). (Republik Indonesia, 2009)

Rekam medis merupakan dokumen yang berisikan data identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang telah diberikan kepada pasien (Kementerian Kesehatan RI, 2022a). Dalam bidang kedokteran, rekam medis adalah satu catatan tertulis terkait dengan kegiatan pelayanan yang diberikan oleh dokter dan dokter gigi, sehingga pencatatan dalam rekam medis harus dilakukan secara benar, lengkap, akurat dan tepat waktu. Mengikuti perkembangan *evidence based medicine* (pelayanan medis berbasis data), diperlukan sebuah data dan informasi pelayanan medis yang berkualitas terintegrasi secara baik dan benar yang bersumber dari data klinis rekam medis, terlebih lagi dengan adanya

perkembangan rekam medis elektronik, setiap entry data secara langsung menjadi masukan (input) dari sistem atau manajemen informasi kesehatan (Konsil Kedokteran Indonesia, 2006).

Rekam medis elektronik adalah rekam medis yang dibuat dengan menggunakan sistem elektronik yang diperuntukkan bagi penyelenggaraan rekam medis (Kementerian Kesehatan RI, 2022). Penyelenggaraan rekam medis elektronik merupakan upaya untuk mencapai penyelenggaraan kesehatan yang cepat, tepat, dan akurat. Akan tetapi dalam penerapannya, rekam medis elektronik tidak luput dari ancaman yang harus diantisipasi oleh setiap pelayanan kesehatan (Ramadhanti, 2021). Salah satu permasalahan dalam penerapan rekam medis elektronik dalam pelayanan kesehatan adalah terkait keamanan data.

Berdasarkan Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi dan aturan dari *ISO/IEC 27001* bahwa keamanan data adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*). Pada keamanan data bidang kesehatan, Menurut Sabarguna (2008) dalam Nugraheni dan Nurhayati (2018) memaparkan bahwa aspek keamanan data terdiri dari enam aspek yaitu *confidentiality*, *integrity*, *authentication*, *availability*, *access control* dan *nonrepudiation*. Dengan aspek *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. *Nonrepudiation* erat kaitannya dengan suatu transaksi atau perubahan informasi. Sebagai sebuah riwayat pendokumentasian, Data kesehatan merupakan data yang menyimpan rekam medis pasien yang bersifat rahasia, sehingga rentan mengalami kebocoran data (Ravlindo, 2021). Click or tap here to enter text.

Roohparvar dalam Direktorat Proteksi Infrastruktur Informasi Kritis Nasional (IIKN) Badan Siber dan Sandi Negara (2019) memaparkan bahwa kemanan informasi pada sektor kesehatan menjadi prioritas utama karena teknik

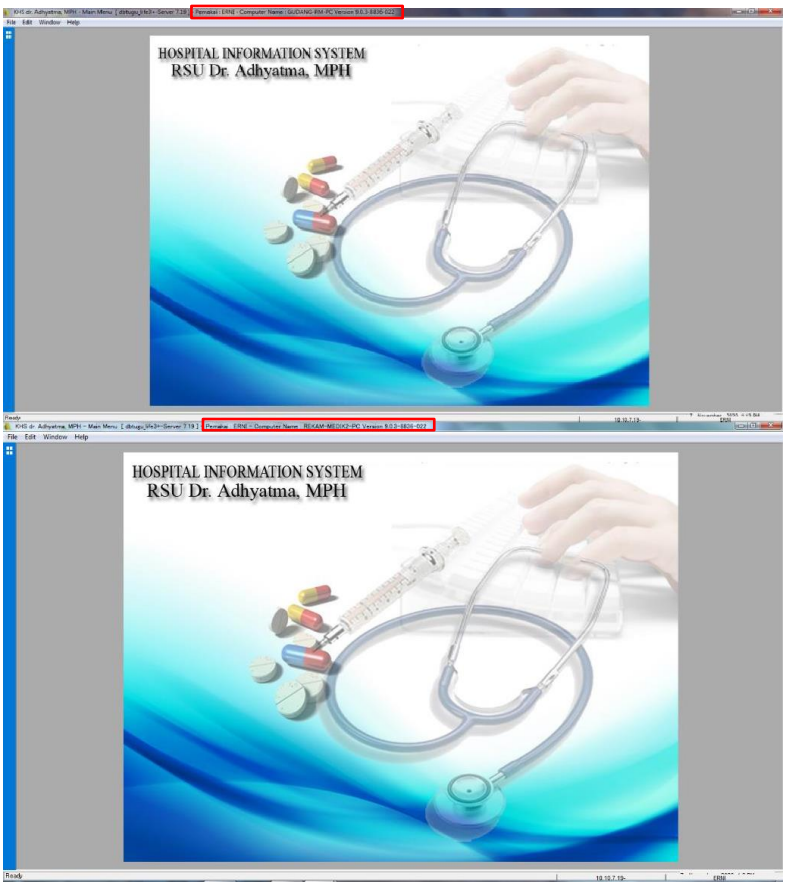
pencurian data oleh hacker semakin variatif, teknik perlindungan sata pasien semakin kompleks, meningkatkannya kasus penyanderaan data menggunakan menggunakan *ransomware*, risiko dari pihak ketiga, kerentanan email dan aplikasi bergerak (*mobile application*). Hal ini semakin diperkuat dengan adanya peretasan data server Kemenkes yang muncul pada forum gelap Raid Forum. Dilansir pada NBC News, peretas mengunakan nama akun Astarte menjual dan membocorkan sebagian data berukuran 720 GB yang berisikan rekam medis di beberapa rumah sakit di Indonesia. Pada data tersebut terdapat file sampel berupa foto-foto pasien korban kecelakaan atau penyakit keras (CNBC 7 Januari 2022). Dampak dari adanya kebocoran riwayat kesehatan mampu mengakibatkan masyarakat memiliki perasaan tidak aman dalam menyimpan informasi data bailk pada instansi pemerintah maupun swasta dikarenakan adanya kerentanan menjadi korban kejahatan *cybercrime* (Zaman et.al., 2021).

Ketentuan terkait dengan keamanan dan kerahasiaan inormasi pada bidang kesehatan diatur dalam *Health Insurance Portability and Accountability Act* (HIPAA) yang harus dipenuhi diantaranya adalah memastikan kerahasiaan, integritas, dan ketersediaan semua informasi kesehatan yang dilindungi dalam membuat, menerima, mempertahankan, atau mentransmisikan informasi kesehatan; Melindungi terhadap ancaman atau bahaya yang diantisipasi secara wajar; Melindungi dari penggunaan atau pengungkapan informasi yang diantisipasi secara wajar berdasarkan peraturan privasi; Pastikan kepatuhan oleh tenaga kerjanya . Ketentuan tersebut dikelompokkan menjadi 3 (tiga) standar keamanan pokok yaitu administrative safeguards (perlindungan administratif), physical safeguards (perlindungan fisik) dan technical safeguards (perlindungan teknis) (Amatyakul, 2013).

RSUD Dr. Adhyatma, MPH Provinsi Jawa Tengah merupakan salah satu rumah sakit yang sudah memulai pengembangan rekam medis elektronik sejak tahun 2005, yang dimulai dari penerapan SIMRS. Seiring berjalannya waktu, Pengimplementasian rekam medis dilakukan secara bertahap yang dimulai dari unit pendaftaran, transaksi pasien pada klinik atau bangsal, farmasi, dan billing (pebayaran). Pengembangan secara bertahap terus berlanjut hingga pada tahun 2017

pelayanan rawat jalan sudah mulai menggunakan rekam medis elektronik. Dengan keberlanjutan pada tahun 2021, secara beriringan pelayanan Rawat Inap dan Instalasi Gawat Darurat mulai mengimplementasikan penggunaan rekam medis elektronik. Hingga akhirnya, saat ini seluruh pelayanan rawat jalan dan beberapa formulir rawat inap serta pelayanan penunjang sudah menggunakan rekam medis elektronik sebagai media penyimpanan data medis pasien. Sehingga, penerapan rekam medis elektronik di RSUD Dr. Adhyatma, MPH perlu dibarengi dengan adanya perlindungan keamanan dan kerahasisaan data pasien.

Berdasarkan hasil pengamatan selama pelaksanaan PKL, ditemukan permasalahan terkait dengan aspek keamanan data informasi pada rekam medis elektronik di RSUD Dr. Adhyatma, MPH Semarang. Hal ini dapat ditinjau dari penggunaan satu akun user yang dapat digunakan secara bersamaan dalam waktu yang sama tanpa adanya pembatasan akses khusus pada *user-id*.



Gambar 1.1 Penggunaan user-id secara bersamaan

Gambar tersebut merupakan tangkapan layar yang diambil dari dua PC yang berbeda, yaitu GUDANG-RM-PC dan REKAM-MEDIK-PC pada hari Selasa, 7 November 2023 pukul 13.13 WIB. Hal tersebut juga didukung oleh adanya saling bertukar informasi terkait dengan *username* dan *password* antar petugas. Sehingga, dikhawatirkan adanya akses akun SIMRS tanpa sepengetahuan pemilik akun. Hal ini sejalan dengan penelitian Tiorentap & Hosizah (2020) bahwa penggunaan satu user-id secara bersamaan dan oleh beberapa orang yang dibarengi dengan antar user yang msaih saling bertukar informasi tidak sesuai dengan aspek *access control* yang menekankan pada pengaturan pembatasan hak akses terhadap informasi. Hal ini akan berakibat fatal jika terjadi kesalahan penginputan, karena menyulitkan proses identifikasi pelaku. Jika hal ini terus berlanjut, dikhawatirkan akan terjadinya penggunaan informasi oleh pihak-pihak yang tidak bertanggungjawab. Pernyataan tersebut juga didukung oleh pernataan informasn yang menyatakan bahwa pernah terjadinya kasus pengisian data medis pasien secara tidak sah pada rekam medis elektronik. Dalam hal ini, pemilik akun tidak merasa melakukan pengisian pada rekam medis elektroik namun riwayat pengisian tertulis nama pemilik akun tersebut. Dampak dari hal tersebut adalah isi dari rekam medis elektronik tersebut tidak dapat dipertangungjawabkan.

Selain itu, masih ditemukannya beberapa formulir rekam medis elektronik yang tidak dilampirkan dengan tanda tangan elektronik. Dalam hal ini, masih adanya pengisian formulir tanpa adanya pembubuhan tanda tangan elektronik. Menurut Ilyas (2023) penggunaan tanda tangan digital pada rekam medis elektronik adalah memberikan autentifikasi dan penjagaan atas privasi terhadap isi atau data medis. Ketiadaan tanda tangan digital menyebabkan rekam medis menjadi tidak berlaku dan tidak mempunyai jaminan yang sah depan hukum, sehingga hal ini dapat mengancam status sosial, psikologis dan jiaw pasien yang ditangani oleh Profesi Pemberi Asuhan (PPA).

Berdasarkan latar belakang yang telah dipaparkan, mengingat pentingnya RSUD Dr. Adhyatma, MPH Semarang 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 untuk menganalisis Aspek Keamanan Data Pada Penerapan Rekam Medik Elektronik Di RSUD Dr. Adhyatma, MPH Provinsi Jawa Tengah.

1.2 Tujuan dan Manfaat

1.2.1 Tujuan Umum MAGANG/PKL

Mengetahui aspek keamanan data pada Sistem Manajemen Informasi Rumah Sakit (SIMRS) dalam pelaksanaan rekam medis elektronik di RSUD Dr. Adhyatma, MPH Semarang.

1.2.2 Tujuan Khusus MAGANG/PKL

a. Menganalisis aspek keamanan data pada penerapan rekam medis elektronik di RSUD Dr. Adhyatma, MPH berdasarkan aspek *confidentialuty*.
b. Menganalisis aspek keamanan data pada penerapan rekam medis elektronik di RSUD Dr. Adhyatma, MPH berdasarkan aspek *integrity.*
c. Menganalisis aspek keamanan data pada penerapan rekam medis elektronik di RSUD Dr. Adhyatma, MPH berdasarkan aspek *authentication*.
d. Menganalisis aspek keamanan data pada penerapan rekam medis elektronik di RSUD Dr. Adhyatma, MPH berdasarkan aspek *availability*.
e. Menganalisis aspek keamanan data pada penerapan rekam medis elektronik di RSUD Dr. Adhyatma, MPH berdasarkan aspek *access control*.
f. Menganalisis aspek keamanan data pada penerapan rekam medis elektronik di RSUD Dr. Adhyatma, MPH berdasarkan aspek *nonrepudiation*.

1.2.3 Manfaat MAGANG/PKL

a. Bagi RSUD Dr. Adhyatma, MPH Semarang

Laporan ini diharapkan dapat menjadi bahan referensi serta pertimbangan dalam proses evaluasi sistem rekam medis elektronik guna meninjau aspek keamanan data secara harfiah.

b. Bagi Politeknik Negeri Jember

Laporan ini diharapkan dapat menjadi bahan referensi dan pembelajaran dan menambah referensi guna menunjang pengembangan ilmu pengetahuan di Politeknik Negeri Jember terkait dengan keamanan data dalam penerapan rekam medis elektronik.

c. Bagi Mahasiswa

Laporan ini diharapkan sebagai bentuk implementasi pengetahuan dalam perkuliahan dan selama melaksanakan kegiatan praktik kerja lapang di RSUD Dr. Adhyatma, MPH, serta menambah pengetahuan mahasiswa terkait keamanan data rekam medis elektronik di RSUD Dr. Adhyatma, MPH Provinsi Jawa Tengah.

1.3 Lokasi dan Waktu

Pelaksanaan Praktik Kerja Lapang dilaksanakan di RSUD Dr. Adhyatma yang beralamat di Jl. Walisongo KM 8,5 No. 137 Semarang, Jawa Tengah yang dilaksanakan pada tanggal 25 September 2023 – 17 Desember 2023.

1.4 Metode Pelaksanaan

1.4.1 Sumber Data

a. Data Primer

Data primer adalah data yang diperoleh secara langsung oleh peneliti (Sugiyono, 2014). Data primer dalam penelitian ini didapatkan dari hasil observasi dan wawancara secara langsung kepada informan yaitu petugas instalasi SIMRS, Petugas Pendaftaran, Pemberi Asuhan Pasien, dan Kepala Instalasi Rekam Medis RSUD Dr. Adhyatma Provinsi Jawa Tengah.

b. Data Sekunder

Data sekunder adalah data yang diperoleh secara tidak langsung yaitu dari hasil pengumpulan orang lain atau melalui dokumen (Sugiyono, 2014). Data sekunder diperoleh melalui jurnal, buku, skripsi penelitian dan internet yang sesuai dengan topik terkait dengan keamanan data pada rekam medis elektronik

1.4.2 Teknik Pengumpulan Data

a. Observasi

Pengamatan yang dilakukan oleh peneliti secara langsung terhadap suatu subjek maupun objek dengan tujuan untuk dapat mengamati dan membandingkan suatu kegiatan, tingkah laku, pengetahuan dan gagasan yang sudah diketahui sebelumnya.

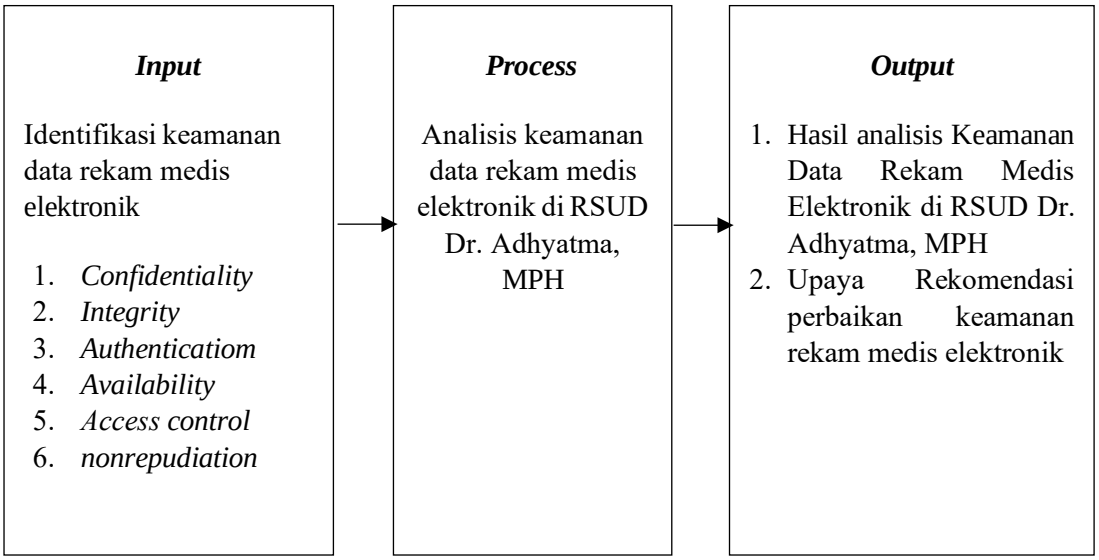
b. Wawancara

Peneliti mengumpulkan dan menggunakan metode wawancara pada variabel *confidentiality, integrity, authentication, availability, access control dan nonrepudiation* untuk menggali informasi secara dalam terkait dengan keamanan data pasien dalam penerapan rekam medis elektronik di RSUD Dr. Adhyatma, MPH Semarang.

c. Dokumentasi

Dokumentasi merupakan sebuah cara yang dilakukan peneliti untuk menyediakan dokumen dengan adanya bukti yang akurat untuk mengetahui kebenaran data. Dokumentasi yang dilakukan peneliti yaitu berupa rekaman, hasil foto, dokumen atau berkas, peraturan-peraturan ataupun data yang relevan dengan penelitian yang didapatkan pada saat sedang melakukan kegiatan penelitian di RSUD Dr. Adhyatma Semarang.

1.5 Kerangka Konsep



Gambar 1.2 Kerangka Konsep Laporan PKL RSUD dr. Adhyatma, MPH Provinsi Jawa Tengah