BAB I
PENDAHULUAN

A. Latar Belakang

Perlindungan informasi data pasien menjadi aspek penting dalam dunia medis, mengingat data tersebut mencakup rincian pribadi yang sangat sensitif seperti identitas, hasil pemeriksaan, diagnosis, hingga riwayat pengobatan. Informasi ini harus dijaga kerahasiaannya dan tidak boleh diakses, digunakan, atau disebarluaskan tanpa izin yang sah. Ketika terjadi kebocoran data, dampaknya bisa sangat merugikan. Bagi pasien, hal ini bisa menimbulkan risiko serius seperti pencurian identitas, kerugian finansial, diskriminasi, hingga pelanggaran hak privasi. Sedangkan bagi institusi pelayanan kesehatan, insiden semacam ini dapat merusak reputasi, mengurangi tingkat kepercayaan masyarakat, dan bahkan berujung pada tuntutan hukum atau sanksi regulator. Oleh karena itu, menjaga keamanan data pasien bukan hanya kewajiban teknis, tetapi juga tanggung jawab etis yang melekat pada penyedia layanan kesehatan (Rani & Widyaningrum, 2024)

Perlindungan terhadap data pasien telah mendapatkan dasar hukum yang kuat melalui sejumlah regulasi, seperti Undang Undang No. 36 Tahun 2009 terkait bidang kesehatan beserta regulasi yang ditetapkan oleh Menteri Kesehatan, peraturan Menteri Kesehatan, serta Undang-Undang Nomor 27 Tahun 2022 terkait dengan upaya perlindungan informasi pribadi. Ketiga regulasi ini memberikan kerangka hukum yang seharusnya mampu menjamin keamanan dan kerahasiaan informasi medis. Namun, dalam pelaksanaannya di lapangan, tantangan masih sering ditemui. Beberapa kendala utama yang dihadapi antara lain keterbatasan infrastruktur teknologi informasi di berbagai fasilitas kesehatan, rendahnya literasi dan kesadaran tenaga kesehatan mengenai pentingnya menjaga privasi data pasien, serta lemahnya sistem penegakan hukum yang membuat pelanggaran terhadap privasi belum mendapatkan sanksi yang tegas dan konsisten (Herisasono, 2024)

Informasi medis yang bersifat pribadi memiliki nilai tinggi dan rentan dimanfaatkan secara tidak semestinya oleh oknum tertentu, sehingga menjaga keamanannya adalah pondasi utama dari sistem kesehatan modern. Upaya perlindungan ini meliputi penerapan teknologi enkripsi, pengaturan akses yang ketat berdasarkan otorisasi, serta pemantauan sistem secara berkelanjutan untuk mengidentifikasi aktivitas mencurigakan (Indra et al., 2024) . Tujuannya bukan hanya menjaga kerahasiaan informasi, tetapi juga memastikan hanya petugas kesehatan dengan hak akses yang diizinkan untuk membuka data tersebut. Kegagalan dalam menjaga keamanan data pasien dapat menimbulkan dampak yang signifikan. Salah satu risiko paling nyata adalah pencurian identitas, di mana informasi medis dan pribadi pasien dapat dimanfaatkan untuk penipuan atau tindak kejahatan lainnya. Selain itu, data medis juga berpotensi disalahgunakan untuk meraih keuntungan pribadi atau bahkan untuk merugikan individu secara profesional maupun pribadi. Situasi ini bukan hanya membahayakan pasien secara langsung, tetapi juga dapat mengikis kepercayaan masyarakat terhadap sistem pelayanan kesehatan secara keseluruhan (Asih et al., 2024).

Dimensi keamanan dalam sistem informasi rekam medis telah diatur secara tegas dalam Peraturan Menteri Kesehatan (Permenkes) No. 24 Tahun 2022, Salah satu tantangan utama adalah rendahnya kesadaran dan pemahaman tenaga kesehatan mengenai pentingnya keamanan data. Banyak tenaga medis yang belum mendapatkan pelatihan khusus tentang keamanan informasi, sehingga mereka mungkin tidak menyadari risiko yang terkait dengan tindakan sehari-hari, misalnya penggunaan password dengan tingkat keamanan rendah atau berbagi informasi pasien melalui saluran yang tidak aman. Hal ini dapat membuka peluang bagi ancaman siber, seperti *phishing* atau penyebaran *malware*, yang bisa membahayakan data pasien. Selain itu, kurangnya infrastruktur teknologi yang memadai di beberapa fasilitas kesehatan juga menjadi kendala. Beberapa institusi mungkin tidak didukung oleh infrastruktur keamanan yang tangguh, contohnya melalui proses enkripsi atau firewall yang efektif, sehingga data pasien menjadi rentan terhadap akses tidak sah (Pokhrel, 2024)

Berdasarkan penelitian (Syauqina et al., 2019) yang dilakukan di sejumlah Puskesmas di Kota Bandung mengungkap bahwa penerapan sistem informasi berbasis komputer dalam pengelolaan data kesehatan, meskipun sudah berjalan secara formal dan didukung oleh kebijakan keamanan informasi, belum sepenuhnya menjamin terbentuknya budaya keamanan informasi yang kuat. Meskipun seluruh Puskesmas dalam penelitian ini telah menerapkan kebijakan keamanan informasi dan menggunakan sistem simpus secara elektronik, pelanggaran dan risiko kebocoran data masih mungkin terjadi, terutama dari sisi kelalaian internal. Temuan lain menunjukkan bahwa meskipun infrastruktur sistem telah siap dan seluruh data dikelola secara elektronik, kesadaran individual belum sepenuhnya terbentuk. Hal ini diperkuat oleh fakta bahwa mayoritas responden merupakan tenaga muda dengan pengalaman kerja 1–5 tahun dan berasal dari latar belakang administrasi atau rekam medis. Dengan demikian, potensi terjadinya kelalaian atau penyalahgunaan akses informasi tetap tinggi jika tidak disertai dengan pemahaman mendalam dan pelatihan berkelanjutan.

Sebagai bagian dari wilayah transformasi layanan kesehatan di Kabupaten Sleman, Puskesmas Gamping 1 dan Puskesmas Gamping 2 telah menerapkan sistem Rekam Medis Elektronik (RME) guna meningkatkan mutu pelayanan dan efisiensi dalam pencatatan data pasien. Kedua puskesmas ini menjadi garda terdepan dalam mendukung digitalisasi sistem informasi kesehatan yang diamanatkan dalam Permenkes No. 24 Tahun 2022.

Puskesmas Gamping 1 telah mulai menggunakan sistem RME sejak Januari 2019. Awalnya menggunakan platform internal bernama Sisfomas, dan kini telah beralih ke sistem SmartHealth yang terintegrasi langsung dengan server Dinas Kesehatan Sleman. Berbagai unit pelayanan seperti poli umum, UGD, poli gigi, KIA, laboratorium, hingga fisioterapi telah aktif memanfaatkan sistem ini. Pengaturan hak akses bagi tenaga kesehatan telah diimplementasikan dengan baik melalui akun pengguna khusus yang dibedakan berdasarkan jabatan. Meskipun demikian, pencadangan data masih dilakukan secara manual, dan belum semua tenaga kesehatan mendapatkan pelatihan khusus mengenai keamanan data digital.

Sementara itu, Puskesmas Gamping 2 yang juga menggunakan sistem SmartHealth menunjukkan komitmen serupa dalam mendukung pelayanan digital. Namun, berdasarkan studi terdahulu dan observasi lapangan, implementasi RME di puskesmas ini belum sepenuhnya optimal. Sebagian modul sistem belum dimanfaatkan maksimal, dan pengisian data masih belum seragam. Evaluasi keamanan data belum dilakukan secara berkala, dan sistem backup masih bersifat manual. Selain itu, pemahaman tenaga kesehatan terhadap aspek integritas dan otorisasi perubahan data masih perlu ditingkatkan. Kondisi di kedua puskesmas ini mencerminkan dinamika yang wajar dalam proses digitalisasi di tingkat layanan primer. Tantangan yang dihadapi bukan merupakan kelemahan institusi, melainkan peluang untuk pengembangan sistem yang lebih aman dan berkelanjutan. Dalam konteks ini, aspek keamanan data menjadi krusial, mengingat RME tidak hanya menyimpan informasi medis, tetapi juga data pribadi pasien yang harus dijaga kerahasiaannya, keutuhannya, dan ketersediaannya.

Oleh karena itu, penting untuk mengetahui sejauh mana pengetahuan tenaga kesehatan tentang keamanan data dalam penerapan RME di Puskesmas Gamping 1 dan 2. Pemahaman ini akan menjadi landasan dalam meningkatkan tata kelola sistem informasi, menyusun kebijakan pelatihan yang tepat, serta memperkuat kepercayaan publik terhadap keamanan informasi dalam layanan kesehatan digital. Penelitian ini diharapkan dapat memberikan kontribusi nyata dalam mendukung pengembangan sistem RME yang tidak hanya canggih, tetapi juga aman, andal, dan sesuai dengan prinsip-prinsip perlindungan data yang berlaku.

B. Rumusan Masalah

Berdasarkan penjelasan latar belakang yang telah disampaikan sebelumnya, permasalahan yang akan diteliti dalam studi ini adalah: “Bagaimana pengetahuan tenaga kesehatan tentang keamanan data pada penerapan rekam medis elektronik di Puskesmas Gamping 1 dan Puskesmas Gamping 2”.

C. Tujuan Penelitian

1. Tujuan Umum

   "Mengidentifikasi pengetahuan tenaga kesehatan tentang keamanan data pada penerapan rekam medis elektronik di Puskesmas Gamping 1 dan Puskesmas Gamping 2."

2. Tujuan khusus
   a. Mengidentifikasi pengetahuan tenaga kesehatan berdasarkan *Kerahasiaan.*
   b. Mengidentifikasi pengetahuan tenaga kesehatan berdasarkan *Integritas.*
   c. Mengidentifikasi pengetahuan tenaga kesehatan berdasarkan *Ketersediaan.*

D. Manfaat Penelitian

1. Manfaat Teoritis
   a. Bagi Institusi Pendidikan

      Diharapkan melalui penelitian ini, dapat memberikan kontribusi dalam proses pengembangan ilmu yang berkaitan dengan rekam medis serta teknologi informasi kesehatan, khususnya yang berkaitan dengan aspek keamanan data dalam penerapan rekam medis elektronik.

   b. Bagi Peneliti Lain

      Temuan dari penelitian ini dapat dijadikan landasan teori untuk studi-studi berikutnya yang ingin mengkaji topik serupa, serta memperkaya literatur akademik tentang pentingnya pengetahuan tenaga kesehatan terhadap keamanan data dalam sistem informasi kesehatan.

   c. Manfaat Praktis
      1) Bagi Peneliti

         Memberikan referensi bagi peneliti dalam memperluas wawasan dan pemahaman mengenai urgensi perlindungan data pada Rekam Medis Elektronik.

2) Bagi Puskesmas Gamping 1 dan Puskesmas Gamping 2

Studi ini diharapkan dapat memberikan kontribusi sebagai dasar pertimbangan dan umpan balik untuk keperluan evaluasi dalam merancang program pelatihan dan edukasi yang lebih efektif untuk meningkatkan pengetahuan tenaga kesehatan mengenai keamanan data.

E. Keaslian Penelitian

Tabel 1. 1 Keaslian Karya Tulis Ilmiah

No	Nama Peneliti & Tahun	Judul Penelitian	Persamaan	Perbedaan
1	I Gusti Agung Ngurah Putra Pradnyantara (2022)	*Readiness of Application of Electronic Medical Records in* RS Bethesda Lempuyangwangi	Sama-sama menggunakan metode kuantitatif deskriptif, serta melibatkan tenaga kesehatan sebagai pengguna sistem RME.	Penelitian ini fokus pada kesiapan organisasi dalam penerapan RME, bukan pada pengetahuan pengguna tentang keamanan data (kerahasiaan, integritas, ketersediaan).
2	Rafi' Abiyyu Mukti (2023)	Analisis Kesiapan Penerapan RME dengan Pendekatan *DOQ-IT*	Menggunakan pendekatan deskriptif analitik, dan membahas pentingnya pelatihan SDM untuk penggunaan RME secara optimal.	Penelitian ini menggunakan kerangka DOQ-IT untuk melihat kesiapan sistem secara menyeluruh, bukan untuk menilai tingkat pengetahuan pengguna tentang aspek keamanan data pasien.
3	Rina Yulida dkk. (2024)	Pengaruh Persepsi Kemudahan terhadap Sikap Profesional Penerapan RME	Sama-sama menggunakan pendekatan kuantitatif, dan melibatkan tenaga kesehatan sebagai responden pengguna RME.	Berfokus pada persepsi dan sikap profesional, bukan pengetahuan keamanan data. Variabelnya bukan kerahasiaan, integritas, atau ketersediaan.
4	Yusrawati & Sri Wahyuni (2015)	Sistem Informasi Rekam Medik Elektronik di RS Bethesda Yogyakarta	Sama-sama meneliti pengguna sistem rekam medis dan proses implementasinya, serta menggunakan pendekatan deskriptif.	Fokus pada prosedur pemberkasan dan alur kerja, bukan pengetahuan individu tenaga kesehatan mengenai keamanan data pasien.
5	Endah Wardani dkk. (2024)	Keamanan Sistem Informasi RME di RS Islam Jakarta Sukapura	Sama-sama membahas aspek keamanan rekam medis elektronik dan menggunakan pendekatan observasional deskriptif.	Fokus penelitian adalah pada kebijakan dan infrastruktur keamanan sistem, bukan pada pengetahuan tenaga kesehatan sebagai pengguna sistem tentang keamanan data.