BAB 2
KAJIAN PUSTAKA

2.1 Rekam Medis Elektronik

Rekam Medis Elektronik adalah catatan medis yang disimpan dalam format digital, berisi informasi pribadi, demografis, sosial, serta data medis pasien dari awal hingga akhir proses pelayanan. RME bersumber dari berbagai data dan berfungsi aktif dalam mendukung pengambilan keputusan klinis secara tepat (Aumar, n.d.).

Menurut (Permenkes No. 24, 2022) Rekam Medis Elektronik adalah catatan medis yang disusun menggunakan sistem digital dan dirancang khusus untuk mendukung proses pengelolaan rekam medis. Sistem elektronik tersebut terdiri dari berbagai perangkat serta prosedur yang berfungsi untuk merancang, menghimpun, memproses, menganalisis, menyimpan, menampilkan, mendistribusikan, mengirim, maupun menyebarkan informasi dalam bentuk elektronik.

Menurut (Permenkes No. 24, 2022) pengaturan rekam medis bertujuan untuk:

1. Meningkatkan mutu pelayanan kesehatan,
2. Memberikan dasar hukum dalam penyelenggaraan dan pengelolaan rekam medis,
3. Menjamin keamanan, kerahasiaan, integritas dan ketersediaan data rekam medis, dan
4. Mewujudkan sistem pengelolaan rekam medis yang berbasis digital dan terintegrasi.

2.1.1 Komponen Rekam Medis Elektronik

Menurut (Mathar, 2018) rekam medis elektronik mempunyai beberapa komponen penting yang mengacu pada kebutuhan yaitu sebagai berikut:

1. Format rekaman

   Bentuk dan struktur rekaman disesuaikan dengan jenis layanan dan kebutuhan rumah sakit.

2. Kinerja sistem

   Sistem harus memungkinkan pencarian cepat, kemudahan dalam memperbarui data, serta stabil digunakan.

3. Kemampuan Pelaporan

   Sistem harus menghasilkan laporan yang akurat, mudah dipahami, dan sesuai standar.

4. Pelatihan dan Pelaksanaan

   Pelatihan/*Training and Implementation* dimana pelatihan yang minimal menggunakan dengan benar. Disini para petugas rekam medis diberikan pengetahuan mengenai penggunaan rekam medis elektronik agar tidak terjadi kesalahan dalam kodefikasi penyakit maupun agar pelayanan yang diberikan menjadi efektif

5. Kontrol dan Akses

   Akses diberikan hanya kepada pihak berwenang seperti dokter dan manajemen, dengan mekanisme pengamanan terhadap penyalahgunaan.

6. *Intelligence*

   Adanya sistem bantu kagatusan, sistem tanda haca yang sesuai dengan yang ditemukan.

7. Keterkaitan Sistem (*Linkages*)

   Sistem RME harus terintegrasi dengan bagian lain seperti manajemen, keuangan, dan basis data pasien.

8. Isi rekaman

   lsi rekaman atau disebut *record content* meliputi standarisasi formulir dan isi, desain formulir, serta sesuai dengan kodefikasi penyakit dan tujuan layanan yang diberikan.

2.2 Keamanan dan Kerahasiaan Data Pasien

Keamanan sistem informasi adalah upaya perlindungan terhadap sistem informasi agar terhindar dari akses, penggunaan, pengungkapan, gangguan, perubahan, pemeriksaan, pencatatan, atau perusakan yang tidak sah. Tujuan utamanya adalah menjaga kerahasiaan, integritas, dan ketersediaan data serta sistem informasi. Keamanan ini mencakup berbagai tindakan pencegahan untuk menghindari pelanggaran yang berkaitan dengan informasi, baik yang tersimpan secara elektronik maupun fisik. Intinya, keamanan sistem informasi bertujuan untuk memastikan bahwa informasi sensitif hanya dapat diakses oleh pihak yang memiliki hak, serta tetap terlindungi dari pihak yang tidak berwenang (Pardosi et al., 2024).

Menurut (Adiba & Oktoriani, 2024) kerahasiaan dan keamanan informasi merupakan aspek yang sangat penting dalam pengelolaan rekam medis yang efektif dan etis. Kerahasiaan mengacu pada perlindungan informasi medis pasien dari

akses yang tidak sah atau pengungkapan yang tidak sah, sementara keamanan berkaitan dengan upaya untuk melindungi data dari kerusakan, kehilangan, atau pencurian. Dalam konteks pengelolaan rekam medis, kerahasiaan dan keamanan informasi merupakan prinsip etika yang mendasar dan juga merupakan keharusan hukum untuk menjaga privasi pasien dan mencegah penyalahgunaan data medis.

Perlindungan privasi pasien adalah aspek sentral dari kerahasiaan informasi dalam pengelolaan rekam medis. Ini berarti bahwa informasi medis pasien harus dijaga kerahasiaan yang tinggi dan hanya diakses oleh individu yang memiliki hak dan kebutuhan untuk mengetahui informasi tersebut untuk memberikan perawatan yang tepat. Selain menjaga kerahasiaan, penting juga untuk memastikan keamanan informasi medis pasien. Sistem keamanan yang baik harus mencakup enkripsi data, pemantauan akses yang ketat, cadangan reguler, dan prosedur pemulihan bencana untuk memastikan bahwa data medis tetap aman dan dapat diakses ketika diperlukan.

2.2.1 Prinsip Utama Keamanan Informasi Dalam Sistem Kesehatan

1. Kerahasiaan (Confidentiality)

Confidentiality berarti informasi dilindungi dari pihak yang tidak berwenang melalui ekripsi dan kontrol akses, untuk menjaga data sensitif indentitas dan riwayat medis pasien. informasi yang harus dijaga kerahasiaannya mencakup data pribadi seperti identitas (misalnya nama lengkap, tanggal lahir), riwayat penyakit, informasi keuangan (seperti nomor kartu kredit), serta data sensitif lainnya seperti nama ibu kandung. Selain itu, data yang dimiliki oleh suatu organisasi atau institusi juga termasuk dalam kategori yang harus dijaga kerahasiaannya. Dalam beberapa kondisi, aspek kerahasiaan (*confidentiality*) dapat berkaitan erat dengan privasi (*privacy*). Tujuan utama dari menjaga kerahasiaan informasi ini adalah:

1. Memberikan pembatasan akses terhadap informasi berdasarkan tingkat sensitivitas data tersebut.
2. Menjamin bahwa data tidak dapat diakses atau diketahui oleh individu atau pihak yang tidak memiliki kewenangan.

Perlindungan terhadap privasi sangat bergantung pada keberadaan sistem yang memiliki tingkat keamanan tinggi. Sistem yang aman mensyaratkan identifikasi yang jelas terhadap setiap individu yang akan mengaksesnya. Fokus utama perlindungan ini terletak pada proses penyampaian informasi dari pasien kepada berbagai tenaga pemberi layanan kesehatan, seperti dokter, perawat, apoteker, dan profesi lainnya yang membutuhkan informasi akurat dan lengkap

guna mendukung pelaksanaan tugas dan pengambilan keputusan klinis (Agustina et al., 2023).

2. Integritas (*Integrity*)

Integritas mengacu pada keutuhan dan keakuratan informasi. Seiring berkembangnya ilmu komputer, kebutuhan data pasien yang tersusun rapi dan mudah diakses semakin meningkat, sehingga mendorong inovasi dalam pengembangan rekam medis elektronnok. Data medis tidak boleh diubah tanpa persetujuan dari pemiliknya, yakni pasien. Kesalahan dalam pencatatan informasi dapat berdampak pada keamanan dan privasi, meskipun secara tidak langsung. Memberikan data yang keliru kepada pihak luar institusi dapat menimbulkan rasa maly dan dianggap sebagai bentuk pemborosan. Kesalahan tersebut juga mencerminkan kegagalan sistem dalam melindungi data secara optimal.

3. Autentikasi *(Authentication)*

Autentikasi merupakan bagian penting dalam menjaga keamanan data pasien, yang bertujuan untuk memastikan bahwa akses terhadap inforasi dalam sistem hanya dapat dilakukan oleh pengguna yang telah terverifikasi dan berwenang. Proses ini dilakukan dengan berbagai metode, seperti penggunaan kata sandi, PIN, biometrik, dan metode lainnya. Selain melalui kombinasi *username* dan *password*, upaya lain untuk meningkatkan perlindungan data pasien adalah dengan menggunakan tanda tangan elektronik. Tanda tangan elektronik merupakan salah satu komponen penting dalam sistem rekam medis elektronik di fasilitas pelayanan kesehatan. Fungsinya tidak hanya sebagai bentuk persetujuan, tetapi juga sebagai sarana validasi terhadap kebenaran isi dokumen medis serta autentikasi identitas

pihak yang memberikan persetujuan tersebut. Oleh karena itu, penggunaan tanda tangan elektronik mendukung aspek legalitas dan keamanan informasi dalam rekam medis elektronik(Widiyanti et al., 2024).

Pentingnya autentikasi pengguna terletak pada fungsinya dalam mencegah akses tidak sah terhadap informasi yang bersifat sensitif. Sebagai ilustrasi, melalui proses autentikasi, seorang pengguna (misalnya A) hanya dapat mengakses data yang sesuai dengan kewenangannya dan tidak dapat melihat informasi pribadi milik pengguna lain (seperti B). Jika metode autentikasi yang digunakan lemah, maka dapat membuka peluang bagi pelaku kejahatan siber untuk menyusup ke dalam sistem dan mencuri data yang dapat menimbulkan kerugian. Salah satu metode perlindungan digital yang dinilai cukup efektif adalah autentikasi dua faktor *(Two-Factor Authentication)***,** yang bekerja dengan mengharuskan pengguna untuk memverifikasi identitasnya menggunakan kata sandi sekali pakai yang dikirimkan oleh server setiap kali terdeteksi adanya upaya akses ke akun (Pardosi et al., 2024).

4. Ketersediaan (*Availability*)

Availability atau ketersediaan adalah aspek yang menekan pada persediaan informasi di dalam organisasi umumnya berlangsung antar unit atau bagian internal. Dalam struktur organisasi seperti rumah sakit, biasanya terdapat seorang manajer yang bertugas mengelola dan mengawasi alur informasi tersebut. Secara hukum, pihak yang bertindak sebagai pengendali data memiliki tanggung jawab untuk memastikan bahwa akses terhadap informasi dilakukan secara terbatas dan tetap menjaga prinsip kerahasiaan, ketersediaan, integritas**,** serta kualitas data yang dikelola.

5. Akses Kontrol (*Acces Control*)

Pengelolaan akses dalam konteks keamanan informasi mengacu pada upaya pengendalian terhadap siapa yang dapat mengakses data, sistem, atau sumber daya informasi tertentu, dengan tujuan mencegah penyalahgunaan akses. Proses ini mencakup penerapan prosedur untuk menjaga kerahasiaan**,** integritas, dan ketersediaan informasi, serta menghindari terjadinya akses ilegal atau penggunaan yang tidak sah. Tujuan utamanya adalah untuk memastikan bahwa hanya individu yang memiliki otorisasi dan tanggung jawab yang tepat yang diperbolehkan mengakses data atau melakukan tindakan tertentu dalam sistem informasi tersebut (Pardosi et al., 2024).

Akses kontrol merupakan elemen penting dalam pengelolaan keamanan informasi, yang berfokus pada mekanisme pengaturan siapa saja yang diperbolehkan atau tidak diperbolehkan mengakses suatu informasi. Melalui proses ini, sistem dapat memastikan bahwa hanya individu yang memiliki wewenang dan alasan yang sah yang dapat mengakses data tertentu. Dalam konteks sistem informasi kesehatan, kontrol akses berperan penting untuk menjamin bahwa data pasien tetap aman dan hanya diakses oleh pihak yang berwenang sesuai dengan tanggung jawabnya.

6. *Non Repudiation*

Non Repudiation atau nirsangkal merupakan aspek penting dalam keamanan informasi yang berkaitan erat dengan transaksi atau perubahan data. Tujuan utama dari aspek ini adalah untuk mencegah pihak tertentu menyangkal telah melakukan suatu tindakan, seperti pengisian atau perubahan informasi.

Adanya mekanisme non-repudiation, setiap aktivitas dapat ditelusuri dan dikaitkan secara jelas dengan identitas pelakunya. Namun, dalam praktiknya, implementasi identifikasi terhadap pihak yang melakukan input maupun perubahan data terkadang belum berjalan secara optimal.

2.3 Unsur 5M

Menurut Harrington Emerson dalam Phiffner John F. dan Presthus Robbert V. (1960) manajemen mempunyai lima unsur (5M). Penyebab hambatan penerapan keamanan dan kerahasiaan rekam medis elektronik dapat dilihat dari aspek *man*, *method*.

1. *Man* (Sumber Daya Manusia)

   Menurun (Effendi, 2014) sumber dara manusia (*Man***)** merupakan faktor penting dalam pelaksanaan RME. Prtugas harus memehami alur kerja sistem dan memiliki kompetensi untuk menjalankan tugas pelayanan secara efektir. Pemahanan yang baik akan sistem elektronik sangat diperlukan untuk mencegah kesalahan dan meningkatkan efisiensi kerja. Hal ini termasuk penempatan orang yang tepat, pembagian kerja, pengaturan jam kerja dan sebagainya.

   Sumber daya manusia merupakan elemen yang memiliki peran strategis dalam pelaksanaan kegiatan organisasi karena memiliki kemampuan berpikir, harapan, dan gagasan yang dapat mengarahkan tercapainya tujuan yang telah direncanakan. Dalam konteks pengelolaan rekam medis elektronik, diperlukan tenaga yang tidak hanya memahami fungsi sistem, tetapi juga mampu menjalankan proses pelayanan kesehatan

dengan memanfaatkan sistem tersebut secara optimal. Oleh karena itu, kualitas dan kompetensi sumber daya manusia menjadi faktor kunci dalam keberhasilan implementasi rekam medis elektronik.

2. *Method* (Prosedur)

   Method merupakan cara sistematis dalam pelaksanaan kerja berdasarkan sasaran, waktu, dan sumber daya yang tersedia. (Rohman, 2017).

3. *Material* (Bahan-bahan)

   Dalam setiap aktivitas sebagian dari proses pelaksanaan manajemen untuk mencapai tujuan yang diterapkan, keberadaan material sangat dibutuhkan. Oleh karena itu, material berperan sebagai sarana atau alat pendukung dalam manajemen.

4. *Money* (Dana)

   Dana adalah pengukuran nilai dari kegiatan yang dapat diukur dari jumlah uang yang telah direncanakan untuk mendukung pelaksanaan suatu kegiatan.

5. *Machine* (Mesin)

   Mesin merupakan pembantu manusia dalam pelaksanaan manajemen untuk mencapai tujuan, bukan sebaliknya manusia sebagai pembantu mesin

2.4 Penelitian Terdahulu

1. Penelitian ini relevan dengan penelitian terdahulu yang diteliti oleh (Ardianto & Nurjanah, 2024) yang berjudul Analisis Aspek Keamanan Data Pasoen Dalam Implementasi Rekam Medis Elektronik Di Rumah Sakit X.

Jenis penelitian yang digunakan dalam penelitian ini adalah kualitatif. Dari penelitian ini dapat disimpulkan:

Aspek keamanan data pasien dalam implementasi rekam medis elektronik sudah terdapat login dan menggunakan *username* dan *password.* Namun masih terdapat beberapa petugas yang belum menggunakan karakter khusus atau kombinasi angka dan huruf dalam penggunaan *password*.

2. Penelitian ini relevan dengan penelitian terdahulu yang diteliti oleh (Tiorentap & Hosizah, 2020) yang berjudul Aspek Keamanan Informasi dalam Penerapan Rekam Medis Elektronik di Klinik Medical Check-Up MP. Metode penelitian yang digunakan adalah penelitian deskriptif kualitatif, dari hasil yang telah diamati dalam penelitian ini, dapat disimpulkan bahwa:

   Aspek kerahasiaan dalam sistem informasi klinik MP diterapkan melalui fitur logout otomatis, di mana sistem akan keluar secara otomatis jika tidak ada aktivitas dari pengguna selama lima menit. Mekanisme ini berfungsi sebagai upaya perlindungan untuk mencegah penyalahgunaan akun pengguna. Namun, efektivitas fitur ini dapat berkurang apabila pengguna mengaktifkan opsi “remember user ID & password”, karena sistem akan menyimpan data akses tersebut secara otomatis, sehingga memungkinkan pihak lain untuk masuk tanpa otorisasi.

3. Penelitian (Widiyanti et al., 2024) yang berjudul Tinjauan Keamanan Data Rekam Medis Elektronik Pada Aplikasi Simpus Berdasarkan Aspek *Confidentiality, Integrity,* dan *Availability* Di Puskesmas Tasikmadu

Karanganyar menyebutkan bahwa keamanan data SIMPUS di puskesmas tasikmadu pada aspek *confidentiality* sudah menggunakan hak *authentication* seperti memiliki *password* dan *username* di setiap bagianya masing-masing sehingga tidak semua orang bisa *login.* Hanya saja SIMPUS belum dilengkapi dengan *automatic log off*. Pada aspek *integrity* sudah dikatakan aman karena data saat diakses bisa diedit oleh pengguna pelayanan dibagiannya saja dan untuk penghapusan data hanya bisa dilakukan oleh admin SIMPUS atau pihak yang bewenang. Pada aspek *availability* saat data dibutuhkan pasti tersedia, dan data SIMPUS juga bisa diakss dimanapun asalkan *user* memiliki hak akses seperti *username* dan *password*, hanya saja belum dilengkapi dengan *back-up* data otomatis tersimpan dikomputer sevr yang hidup 24 jam.

4. Pada penelitian (Wardani et al., 2024) menyebutkan bahwa di Rumah Sakit Islam Jakarta Sukapura belum sepenuhnya memiliki SOP khusus untuk mengatur keamanan sistem informasi rekam medis elektronik. Meskipun terdapat SOP Nomor 33 yang mengenai Perlindungan Rekam Medis Dari Pengguna/Akses Tidak Sah, terdapat ketidaksesuaian antara isi SOP dan praktik di lapangan. Pada aplikasi SIMRS terdapat toga aspek keamanan yang belum terlaksana dengan baik, yaitu aspek privasi (fitur otomatis*logout*), aspek ketersediaan (ketersambungan dengan satu sehat), aspek tidak ada penlokan riwayat perubahan data). Dapat disumpulkan bahwa aplikasi SIMRS milik rumah sakit islam jakarta sukapura belum

memenuhi standar keamanan yang seharusnya ada dalam sistem informasi kesehatan.

5. Pada penelitian (Soraya et al., 2025) yang berjudul Evaluasi Keamanan dan Privasi Sistem Rekam Medis Elektronik: Studi Kasus Di Rumah Sakit Wava Husada tahun 2025 menyebutkan bahwa Rumah Sakit Wava Husada telah mampu menerapkan aspek kerahasiaan yang meliputi penggunaan *username* dan *password*, *automatic log off*, dan penanganan nomor ganda. Pada aspek integritas telah menerapkan perubahan atau penghapusan data, dan pengawasan data. Pada aspek autentikasi telah menerapkan penggunaan hak akses yang tepat dan kebijakan hak akses. Pada aspek ketersediaan telah menerapkan ketersediaan data, penggunaan backup data, ketersediaan data dalam sistem. Pada aspek akses kontrol telah menerapkan penggunaan *password* dan *username*, pembatasan hak akses,dan pelatihan staf tentang pentingnya akses kontrol. Pada aspek nir sangkal telah mampu menerapkan pengidendifikasi pihak yang melakukan akses, log file untuk pemantauan.
6. Pada penelitian (Suhariyono et al., 2025) yang berjudul Analisis Aspek Keamanan Informasi Data Pasien pada Rekam Medis Elektronik di UPT Puskesmas Karangploso menyebutkan bahwa pada aspek keamanan data pasien dalam implementasi rekam medis elektronik berdasarkan aspek kerahasiaan sudah menggunakan *username* dan *password* saat *login* ke aplikasi E-Puskesmas pada bagiannya masing-masing dan setiap user dilengkapi dengan fitur *log out* otomatis. Pada aspek integritas sudah dapat melakukan pengeditan data saat diakses oleh pengguna pelayanan di

bagiannya saja dan untuk penghapusan atau perubahan data yang besar hanya bisa dilakukan oleh pihak petugas rekam medis dan petugas IT selaku administrator layanan. Pada aspek ketersediaan sudah menunjang keamanan data karena saat data dibutuhkan pasti sangat cepat tersedia, puskesmas juga memiliki ketersediaan daya internet yang sangat itnggi, dan penyimpanan data dilakukan menggunakan *database*. Dimana akan tersimpan otomatis di *database* dan tidak ada risiko hilang selama 25 tahun.