

# **Analisis Aspek Keamanan Informasi Data Pasien pada Rekam Medis Elektronik di UPT Puskesmas Karangploso**

**Untung Slamet Suhariyono<sup>1</sup>, Fita Rusdian Ikawati<sup>2</sup>, Nur Afifah<sup>3\*</sup>**

<sup>1</sup>Program Studi D-III Rekam Medis dan Informasi Kesehatan,  
Institut Teknologi Sains dan Kesehatan RS dr. Soepraoen Malang

E-mail: <sup>1</sup>untungslamet@itsk-soepraoen.ac.id

<sup>2,3</sup>Program Studi D-III Rekam Medis dan Informasi Kesehatan,  
Institut Teknologi Sains dan Kesehatan RS dr. Soepraoen Malang  
E-mail: <sup>2</sup>fita.160978@itsk-soepraoen.ac.id, <sup>3</sup>fifahnur2002@gmail.com

## **Abstract**

*Electronic Medical Records (EMR) serve as evidence of the implementation of information technology in healthcare services. To ensure the security of information in electronic medical records, Indonesian Ministry of Health Regulation No. 24 of 2022 on Medical Records, Article 29, outlines three key aspects: confidentiality, integrity, and availability. The objective of this study is to examine data security at Karangploso Community Health Center (Puskesmas Karangploso). This research employs a descriptive qualitative approach. The subjects of the study are users who have access to electronic medical records at Puskesmas Karangploso, while the object is the E-Puskesmas application. The instruments used in this study include interview guidelines and observation guidelines. Data collection was carried out through observation and interviews. The data processing techniques in this research involve data collection, data reduction, data presentation, and conclusion drawing. The analysis used is descriptive. The results of the study focus on the security of electronic medical record data in the E-Puskesmas application based on the aspects of confidentiality, integrity, and availability at Puskesmas Karangploso. In terms of confidentiality, data security is maintained as staff members are required to log in to the E-Puskesmas application using their respective usernames and passwords. Regarding integrity, data security is ensured because data can only be edited by users in their respective sections, and major data deletions or modifications can only be performed by authorized personnel. For availability, data security is also guaranteed, as necessary data can be accessed quickly, and electronic medical records are securely stored in the database without risk of loss for up to 25 years. The conclusion of this study highlights the importance of healthcare facilities in safeguarding patient data within the implementation of electronic medical records, as well as the potential consequences if patient medical record information is leaked and misused by unauthorized parties.*

**Keywords:** Security Data, Confidentiality, Integrity, Availability.

## **Abstrak**

Rekam Medis Elektronik merupakan salah satu bukti penerapan teknologi informasi dalam layanan kesehatan. Dalam upaya menjaga keamanan informasi data pada rekam medis elektronik, Permenkes RI 24 Tahun 2022 tentang Rekam medis pasal 29 yang mencakup tiga aspek, yaitu *confidentiality, integrity, availability*. Tujuan penelitian ini adalah untuk mengetahui keamanan data di Puskesmas Karangploso. Jenis penelitian yang digunakan adalah deskriptif dengan pendekatan kualitatif. Subjek penelitian ini adalah pengguna yang memiliki akses terhadap rekam medis elektronik di Puskesmas Karangploso, sedangkan objeknya adalah aplikasi E-Puskesmas. Instrumen yang digunakan dalam penelitian ini adalah pedoman wawancara dan pedoman observasi. Pengumpulan data dilakukan melalui observasi dan wawancara. Teknik pengolahan data dalam penelitian ini meliputi pengumpulan data, reduksi data, penyajian data, dan penarikan kesimpulan. Analisis yang digunakan bersifat deskriptif. Hasil penelitian mengenai keamanan data rekam medis elektronik pada aplikasi E-Puskesmas berdasarkan aspek *confidentiality, integrity, dan availability* di Puskesmas Karangploso. Keamanan data pada aspek *confidentiality* terjaga dimana saat *log-in* ke aplikasi E-Puskesmas petugas sudah menggunakan *username* dan *password* disetiap bagiannya masing-masing. Pada aspek *integrity* keamanan datanya dinyatakan aman karena data hanya bisa diedit oleh pengguna di bagian masing-masing dan untuk penghapusan atau perubahan data yang besar data hanya dilakukan oleh pihak yang berwenang. Dalam aspek *availability*, keamanan data juga terjamin karena saat data diperlukan, data tersebut dapat diakses dengan cepat, dan data rekam medis akan tersimpan aman

di *database* tanpa ada risiko kehilangan selama 25 tahun. Kesimpulan dari penelitian ini adalah pentingnya fasilitas kesehatan dalam menjaga keamanan data 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.

**Kata kunci:** Keamanan Data, Confidentiality, Integrity, Availability.

## PENDAHULUAN

Menurut Permenkes Nomor 43 Tahun 2019 tentang Pusat Kesehatan Masyarakat yang biasa disebut Puskesmas adalah fasilitas pelayanan kesehatan yang menyelenggarakan Upaya Kesehatan Masyarakat (UKM) dan Upaya Kesehatan Perseorangan (UKP) tingkat pertama, dengan lebih mengutamakan upaya promotif dan preventif di wilayah kerjanya (Permenkes, 2019).

Dalam era digital saat ini, pemanfaatan teknologi informasi dalam sektor kesehatan semakin meningkat, salah satu inovasi yang signifikan adalah penerapan rekam medis elektronik (RME) di Puskesmas. Rekam medis elektronik Fasilitas penyedia layanan kesehatan, salah satu yang termasuk memanfaatkan kemajuan teknologi untuk memberikan layanan kepada pasien, salah satu sistem informasi manajemen di puskesmas Karangploso. Data kesehatan, terutama rekam medis pasien bersifat sangat rahasia sehingga rentan terhadap kebocoran. Sebagaimana di atur dalam Permenkes RI Nomor 24 Tahun 2022 tentang Rekam medis pasal 29 keamanan dan perlindungan data yang meliputi: kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) yang digunakan sebagai peningkatan penggunaan sistem rekam medis elektronik (Permenkes, 2022).

Menurut Permenkes RI Nomor 31 Tahun 2019 tentang Sistem Informasi Manajemen Puskesmas (SIMPUS) adalah suatu tatanan yang menyediakan informasi untuk membantu proses pengambilan keputusan dalam melaksanakan manajemen puskesmas (Permenkes 2019). Keamanan data adalah jaringan entitas yang berkomunikasi yang dapat dibuat dengan berbagai cara, seperti perutean, kebijakan kontrol akses atau yang mungkin termasuk pelabelan yang meliputi bagaimana sistem diberi label sehingga mampu mengekspresikan banyak jenis persyaratan keamanan menurut Qamaddin (2020). Disisi lain keamanan secara umum dapat didefinisikan sebagai pembatasan akses terhadap informasi pribadi, yang hanya diberikan kepada pihak-pihak yang berwenang menurut Ikawati & Ansyori, (2023).

Menurut Peraturan Arsip Nasional RI Nomor 15 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi di Lingkungan Arsip Nasional Indonesia, keamanan informasi berarti menjaga kerahasiaan, keutuhan, dan ketersediaan informasi. Hubungan antara SIMPUS dan keamanan sistem pada dasarnya sama dengan menjamin kerahasiaan organisasi.

Puskesmas Karangploso telah menggunakan aplikasi E-Puskesmas sejak tahun 2018 diperoleh dari vendor. Untuk perkembangan teknologi informasi mendorong untuk pengembangan sistem rekam medis elektronik pada sistem aplikasi E-Puskesmas, sehingga pada bulan Oktober 2023 rekam medis elektronik (RME) mulai diimplementasikan pada instalasi rawat jala. Sistem ini dapat digunakan untuk pendaftaran pasien, dokumentasi rekam medis, daftar kunjungan pasien, pembayaran, stok barang dan obat-obatan, serta laporan karena sudah terintegrasi dengan aplikasi penunjang medis. Puskesmas Karangploso masih melakukan secara manual seperti tanda tangan persetujuan kunjungan dan rekam medis di pelayanan rawat inap.

Hasil studi pendahuluan di Puskesmas Karangploso menunjukkan aspek *confidentiality* dimana saat *log-in* ke aplikasi E-Puskesmas petugas sudah menggunakan *username* dan *password* disetiap bagiannya masing-masing. Di bagian aspek *integrity* keamanan datanya sudah dikatakan aman karena data hanya bisa di edit pengguna pelayanan di bagiannya saja dan untuk penghapusan data hanya dilakukan oleh pihak yang berwenang. Dibagian *availability* dimana dalam aspek ini sudah menunjang untuk keamanan datanya dikarenakan saat data dibutuhkan pasti dengan cepat tersedia, dan data rekam medis akan tersimpan aman di *database* dan tidak akan hilang sampai waktu 25 tahun.

Berdasarkan latar belakang ini, pentingnya fasilitas kesehatan dalam menjaga keamanan data pasien dalam pelaksanaan rekam medis elektronik, serta dampak yang ditimbulkan jika informasi bocor dan beresiko disalahgunakan oleh pihak yang tidak bertanggung jawab.

## METODE

Jenis penelitian ini adalah deskriptif dengan pendekatan kualitatif, yang bertujuan untuk menggambarkan dan menganalisis keamanan data rekam medis elektronik pada aplikasi E-Puskesmas berdasarkan aspek *confidentiality*, *integrity*, dan *availability* di Puskesmas Karangploso. Penelitian ini dilaksanakan di bagian pendaftaran rekam medis rawat jalan Puskesmas Karangploso.

Penelitian ini dilakukan pada bulan Oktober 2024-Januari 2025. Subjek penelitian ini terdiri dari seluruh pengguna yang memiliki akses terhadap rekam medis elektronik, sedangkan objek penelitian ini adalah aplikasi E-Puskesmas di Puskesmas Karangploso. Penelitian ini menggunakan teknik pengambilan sampel *nonprobability sampling* dengan Pendekatan *purposive sampling*, yaitu menentukan sampel berdasarkan kriteria atau pertimbangan tertentu, sehingga diperoleh sampel sebanyak 4 informan yaitu, kepala rekam medis, petugas IT, petugas pendaftaran rawat jalan, perawat.

Instrumen penelitian yang digunakan adalah pedoman observasi berupa *check list* sebagai alat untuk mengetahui aspek keamanan data pasien pada rekam medis elektronik rawat jalan di Puskesmas Karangploso, serta pedoman wawancara digunakan sebagai alat untuk memperoleh data maupun informasi yang dirangkum dalam bentuk pertanyaan secara umum. Pengumpulan data dilakukan melalui observasi, dan pengambilan informasi melalui pengamatan secara langsung dan wawancara secara umumnya. Teknik pengumpulan data yang dilakukan meliputi, reduksi data, penyajian data, dan penarikan kesimpulan.

## HASIL

### Keamanan Data Pasien Pada Aspek Kerahasiaan (*Confidentiality*)

Menurut Permenkes RI Nomor 24 Tahun 2024 tentang Rekam medis pasal 29 menjelaskan aspek keamanan kerahasiaan (*confidentiality*) merupakan jaminan keamanan data dan informasi dari gangguan pihak internal maupun eksternal yang tidak memiliki hak untuk mengakses. Berdasarkan aspek *confidentiality* keamanan data pasien pada rekam medis elektronik di Puskesmas Karangploso hanya dapat diakses menggunakan *username* dan *password* setiap masing-masing petugas.

#### a) Penggunaan *Username* dan *Password*

Berikut ini merupakan hasil wawancara dengan informan terkait penggunaan *username* dan *password* di Puskesmas Karangploso:

*"Petugas IT dan perekam medis di sini untuk melindungi data rekam medis, hanya petugas IT dan petugas rekam medis yang dapat mengakses data rekam medis. Setiap petugas sudah menggunakan username dan password masing-masing"* (W-KRM).

Hanya petugas rekam medis dan petugas IT yang memiliki hak akses untuk mengganti *username* dan *password* setiap 3 bulan, bertujuan untuk menjaga keamanan data. Setiap petugas diberikan *username* dan *password* untuk memastikan keamanan akses.

Hasil dalam wawancara di Puskesmas Karangploso, setiap pengguna rekam medis elektronik memiliki *username* dan *password* masing-masing. *Ussername* dan *password* ini dibuat oleh kepala rekam medis dan petugas IT di Puskesmas. Sebagai salah satu upaya dalam menjaga keamanan data pada sistem rekam medis elektronik, dan dilakukan perubahan *password* setiap 3 bulan sekali untuk memastikan keamanan data di aplikasi E-Puskesmas sesuai dengan ketentuan dari administrator sistem.

#### b) Fitur *Log Out* Otomatis

Berikut ini merupakan hasil wawancara dengan informan terkait adanya fitur *log out* otomatis dalam sistem E-Puskesmas di Puskesmas Karangploso:

*"Ya ada, sistem bisa log out otomatis, kayaknya sih sekitar 5 menit. Jika ditinggal kemana-mana gitu masih bisa kurang lebih satu jaman"* (W-KRM)

Untuk menjaga keamanan *username* dan *password* sangat penting agar informasi tersebut tidak bocor atau diketahui orang lain. Jika tidak ada aktivitas di aplikasi selama beberapa menit, pengguna diwajibkan untuk melakukan login ulang untuk dapat mengakses di aplikasi.

Hasil dalam wawancara di Puskesmas Karangploso menunjukkan bahwa sistem rekam medis elektronik telah dilengkapi dengan fitur *log out* otomatis untuk menjaga *username* dan *password* kita aman

dan tidak sampai bocor atau diketahui orang lain. Dimana jika pengguna tidak melakukan aktivitas dalam waktu kurang lebih 5 menit. Fitur *log out* otomatis pada sistem rekam medis elektronik di Puskesmas Karangploso aktif tetapi memiliki waktu lebih lama selama 1 jam setelah adanya aktivitas yang dilakukan.

Berdasarkan hasil penelitian di Puskesmas karangploso menunjukkan bahwa keamanan data pasien dari aspek *confidentiality* sudah sesuai karena sudah ada *username* dan *password*, untuk setiap *user* telah memiliki fitur *log out* otomatis dalam waktu kurang lebih selama satu jam setelah tidak adanya aktivitas yang dilakukan di dalam sistem rekam medis elektronik.

### **Keamanan Data Pasien Pada Aspek Integritas (*Integrity*)**

Menurut Permenkes RI Nomor 24 Tahun 2022 tentang Rekam medis pasal 29 menjelaskan bahwa aspek keamanan integritas (*integrity*) merupakan keakuratan data dan informasi yang ada dalam rekam medis elektronik, dan perubahan terhadap data hanya boleh dilakukan oleh orang yang diberi hak akses untuk mengubah dan bisa dipertanggungjawabkan.

Berdasarkan hasil wawancara dan observasi pada rekam medis elektronik di aplikasi E-Puskesmas terkait pengeditan, perubahan dan penghapusan data di Puskesmas Karangploso:

*“Ya, yang bisa melakukan penghapusan atau perubahan data yang besar dilakukan oleh kepala rekam medis dan petugas IT, selaku administrator layanan disini”* (W-IT)

Kepala rekam medis dan petugas IT tidak dapat mengubah atau memalsukan data. Pengeditan data hanya dapat dilakukan oleh pengguna dibagian masing-masing dengan mengeklik tombol edit. Pengguna memiliki batas waktu 1x24 jam untuk melengkapi atau mengedit data setelah pasien selesai pengobatan.

Hasil penelitian di Puskesmas Karangploso terkait keamanan data pada aplikasi E-Puskesmas di tinjau berdasarkan aspek *integrity* dimana saat pengeditan data di E-Puskesmas bisa dilakukan di bagiannya masing-masing saja seperti perawat hanya bisa mengedit di bagian kolom perawat, dokter hanya bisa mengedit di bagiannya saja dan saat pengeditan data atau melengkapi di bagian kolom dengan

waktu 1x24 jam setelah pasien selesai melakukan pengobatan. Tetapi untuk penghapusan atau perubahan data yang besar dilakukan oleh kepala rekam medis dan petugas IT yang berwenang atau selaku administrator pelayanan di Puskesmas.

### **Keamanan Data Pasien pada Aspek Ketersediaan (*Availability*)**

Menurut Permenkes RI Nomor 24 Tahun 2022 tentang Rekam medis pasal 29 menjelaskan bahwa ketersediaan merupakan jaminan data dan informasi yang ada dalam rekam medis elektronik dapat diakses dan digunakan oleh orang yang telah memiliki hak akses yang ditetapkan oleh pimpinan pelayanan kesehatan.

Berdasarkan hasil wawancara dan observasi pada rekam medis elektronik terkait ketersediaan dan penyimpanan data pada aplikasi E-Puskesmas di Puskesmas Karangploso:

*“Disini sudah disediakan genset yang otomatis menyala jika suatu saat PLN padam sehingga tidak terjadi sistem downtime”* (W-KRM)

Di Puskesmas Karangploso ini juga tersedia koneksi internet yang sangat tinggi, memudahkan pengiriman data pasien saat dibutuhkan sewaktu-waktu. Puskesmas bekerjasama dengan Dinas Kesehatan dan menggunakan aplikasi E-Puskesmas, sehingga penyimpanan data dilakukan di *database* dinas atau infokes. Penerapan rekam medis lektronik ii memudahkan penginputan data yang otomatis tersimoan di *database* dan terjamin tidak akan hilang selama 25 tahun.

Hasil penelitian di Puskesmas Karangploso terkait ketersediaan dan penyimpanan data pada aplikasi E-Puskesmas, ditinjau dari aspek keamanan *availability* menunjukkan bahwa ketersediaan di puskesmas telah disediakan genset otomatis yang akan menyala jika aliran listrik dari PLN padam. Sehingga pada saat pelayanan tetap dapat berjalan tanpa mengalami sistem *downtime*. Selain itu, puskesmas juga memiliki ketersediaan daya internet yang sangat tinggi, sehingga saat membutuhkan data pasien dapat diakses dengan cepat. Puskesmas telah bekerjasama dengan dinas kesehatan dan menggunakan aplikasi E-Puskesmas, sehingga penyimpanan data dilakukan melalui *database*. Data akan tersimpan secara otomatis, sehingga tidak ada risiko kehilangan selama 25 tahun.

## PEMBAHASAN

### Keamanan Data Pasien Pada Aspek Kerahasiaan (*Confidentiality*)

Berdasarkan hasil penelitian di Puskesmas Karangploso menunjukkan bahwa keamanan data pasien dari aspek *confidentiality* sudah sesuai karena sudah ada *username* dan *password* untuk setiap *user* telah memiliki fitur *log out* otomatis dalam waktu kurang lebih selama satu jam setelah tidak adanya aktivitas yang dilakukan di dalam sistem rekam medis elektronik.

#### a) Penggunaan *Username* dan *Password*

Berdasarkan hasil penelitian di Puskesmas Karangploso, setiap pengguna rekam medis elektronik memiliki *username* dan *password* masing-masing. *Username* dan *password* ini dibuat oleh kepala rekam medis dan petugas IT di Puskesmas. Sebagai salah satu upaya dalam menjaga keamanan data pada sistem rekam medis elektronik, dan dilakukan perubahan *password* setiap 3 bulan sekali untuk memastikan keamanan data di aplikasi E-Puskesmas sesuai dengan ketentuan dari administrator sistem.

Hal ini juga sudah sesuai dengan penelitian Sofia *et.al.*, (2022), bahwa fasilitas kesehatan untuk menjaga keamanan rekam medis elektronik dalam memastikan aspek *confidentiality* meliputi penerapan *login* menggunakan *username* dan *password*, penerapan *automatic log off*, penggunaan teknologi kriptografi, dan pemblokiran akses ke data melalui teknologi jaringan.

#### b) Fitur *Log Out* Otomatis

Hasil penelitian di Puskesmas Karangploso menunjukkan bahwa sistem rekam medis elektronik telah dilengkapi dengan fitur *log out* otomatis, jika pengguna tidak melakukan aktivitas dalam waktu kurang lebih 5 menit. Fitur *log out* otomatis pada sistem rekam medis elektronik di Puskesmas Karangploso aktif tetapi memiliki waktu lebih lama selama 1 jam setelah adanya aktivitas yang dilakukan.

Hal ini juga sudah sesuai dengan penelitian Tiorentap *et.al.*, (2020), menyatakan bahwa aspek *confidentiality* diperkuat dengan tidak adanya (melakukan *log out* secara otomatis) sistem informasi Klinik MP jika tidak ada

aktivitas yang dilakukan oleh *user* dalam waktu 5 menit. Fitur ini berfungsi untuk melindungi dan mencegah penyalahgunaan *user id*. Namun jika *user* melakukan *log in* dengan tindakan “remember *user id* dan *password*” hal ini tidak akan efektif karena sistem akan menyimpan data dan akan memudahkan setiap orang *log in*.

Seperti halnya yang dinyatakan oleh Sofia *et.al.*, (2022) bahwa aspek *confidentiality* dibuktikan dengan bentuk tidak berfungsinya (melakukan *log out* otomatis) sistem rekam medis elektronik di klinik jika dalam kurun waktu 5 menit tidak terjadi aktivitas yang dilakukan oleh *user*. Penggunaan fitur *log out* otomatis berfungsi sebagai salah satu bentuk pertahanan dalam penyalahgunaan *username*. Bentuk dari perlindungan dengan adanya fitur *log out* otomatis di Puskesmas Karangploso sudah sesuai dengan teori menurut Sofia *et.al.*, (2022).

Suatu sistem informasi sebaiknya juga memiliki fitur yang memungkinkan pengguna keluar (*log out*) otomatis apabila tidak ada aktivitas yang dilakukan dalam jangka waktu tertentu. Fitur *log out* otomatis sangat penting untuk mencegah orang yang tidak berhak mengakses sistem, jika *user* keluar meninggalkan sistem dalam keadaan terbuka.

### Keamanan Data Pasien pada Aspek Integritas (*Integrity*)

Hasil penelitian di Puskesmas Karangploso terkait keamanan data pada aplikasi E-Puskesmas di tinjau berdasarkan aspek *integrity* dimana saat pengeditan data di E-Puskesmas bisa dilakukan di bagianya masing-masing saja seperti perawat hanya bisa mengedit di bagian kolom perawat, dokter hanya bisa mengedit di bagianya saja dan saat pengeditan data atau melengkapi di bagian kolom dengan waktu 1x24 jam setelah pasien selesai melakukan pengobatan. Tetapi untuk penghapusan data hanya berhak dilakukan oleh kepala rekam medis dan petugas IT yang berwenang atau selaku administrator pelayanan di Puskesmas.

Hal ini sesuai dengan penelitian yang dilakukan oleh Rahmadiliyani (2018) menjelaskan bahwa RSUD Ratu Zalescha Martapura bahwa perubahan yang bersifat besar harus mengkonfirmasi kepada bagian IT dan bagian IT yang akan melakukan perubahan dengan sepengetahuan semua pihak yang terlibat. Dalam penelitian ini *integrity* dapat dilihat dari

adanya fitur edit dan hapus yang dapat digunakan untuk mengubah data pasien dalam sistem rekam medis elektronik. Hal ini sesuai dengan penelitian yang dilakukan oleh Hidayah (2023) menjelaskan bahwa RSUP Nasional Dr. Cipto Mangkusumo Jakarta apabila dokter ingin melakukan perubahan isi dari rekam medis elektronik memerlukan persetujuan dari bagian rekam medis yaitu kepala sub bagian rekam medis, penanggung jawab pelayanan rekam medis, dan kepala instalasi rekam medis dan administrator.

### **Keamanan Data Pasien pada Aspek Ketersediaan (*Availability*)**

Hasil penelitian di Puskesmas Karangploso terkait ketersediaan dan penyimpanan data pada aplikasi E-Puskesmas, ditinjau dari aspek keamanan *availability* menunjukkan bahwa ketersediaan di puskesmas telah disediakan genset otomatis yang akan menyala jika aliran listrik dari PLN padam. Sehingga pada saat pelayanan tetap dapat berjalan tanpa mengalami sistem *downtime*. Selain itu, puskesmas juga memiliki ketersediaan daya internet yang sangat tinggi, sehingga saat membutuhkan data pasien dapat diakses dengan cepat. Puskesmas telah bekerjasama dengan dinas kesehatan dan menggunakan aplikasi E-Puskesmas, sehingga penyimpanan data dilakukan melalui *database*. Data akan tersimpan secara otomatis, sehingga tidak ada risiko kehilangan selama 25 tahun.

Hal ini sesuai dengan penelitian yang dilakukan oleh Nugraheni (2018) menjelaskan ketersediaan (*Availability*) adalah aspek yang menekankan pada tersedianya informasi saat diakses oleh pihak-pihak yang terkait. Sebagai alat komunikasi, rekam medis harus selalu dapat diakses dengan cepat dan dapat menampilkan kembali data yang telah tersimpan sebelumnya.

### **SIMPULAN**

Aspek kerahasiaan (*Confidentiality*), dapat disimpulkan bahwa aspek keamanan data pasien dalam implementasi rekam medis elektronik dimana saat *log in* ke aplikasi E-Puskesmas sudah menggunakan *username* dan *password* di setiap bagiannya masing-masing sehingga tidak semua orang bisa *log in* dan setiap *user* sudah dilengkapi dengan fitur *log out* otomatis

Aspek integritas (*Integrity*), dapat disimpulkan dimana dalam aspek ini sudah sudah dikatakan aman karena data saat diakses bisa diedit 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.

Aspek ketersediaan (*Availability*), dapat disimpulkan dimana dalam aspek ini sudah menuju keamanan data karena saat data dibutuhkan pasti sangat cepat tersedia, karena puskesmas juga memiliki ketersediaan daya internet yang sangat tinggi, dan penyimpanan data dilakukan menggunakan *database*. Dimana data akan tersimpan secara otomatis di *database* dan tidak ada risiko hilang selama 25 tahun.

### **UCAPAN TERIMA KASIH**

Peneliti mengucapkan terima kasih kepada staf di Puskesmas Karangploso yang telah memfasilitasi pelaksanaan penelitian ini. Selain itu peneliti ingin mengucapkan terima kasih kepada IITSK dr. Soepraoen Malang yang telah membantu terselesaikannya laporan penelitian dan jurnal penelitian ini.

### **DAFTAR PUSTAKA**

- Berita, N. R. I. Nomor 24 Tahun 2022 tentang *Rekam Medis*. 31 Agustus 2022. Jakarta
- Gandana, D. (2022). IMPLEMENTASI PERATURAN MENTERI KESEHATAN NOMOR 43 TAHUN 2019 TENTANG PUSAT KESEHATAN MASYARAKAT (Studi di UPTD Puskesmas Cikalang Kabupaten Tasikmalaya). *Indonesian Journal of Education and Humanity*, 2(4), 197-203.
- Hidayah, E. N. (2023). Analisis Aspek Keamanan Data pada Hospital Information System (HIS) dalam Penerapan Rekam Medis Elektronik di RSUP Nasional Dr. Cipto Mangunkusumo Jakarta.
- Ikawati, F. R., & Ansyori, A. (2023, May). TANTANGAN REKAM MEDIS ELEKTRONIK DALAM PERLINDUNGAN DATA PRIBADI CHALLENGES OF ELECTRONIC MEDICAL RECORDS IN PERSONAL DATA PROTECTION. In *PROSIDING SEMINAR NASIONAL REKAM MEDIS & MANAJEMEN INFORMASI KESEHATAN*.

- Kemenkes, RI (2019). Peraturan Menteri Kesehatan No. 31 Tahun 2019 tentang Sistem Informasi Puskesmas. Tersedia di <https://peraturan.bpk.go.id/Beranda/Detail/138622/permendikbud-no-31-tahun-2019>.
- Kementerian Kesehatan, (2021). Kepmenkes Peraturan Arsip Nasional Republik Indonesia Nomor 15 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi di Lingkungan Arsip Nasional Republik Indonesia. <https://peraturan.bpk.go.id/Details/192824/peraturan-anri-no-15-tahun-2021>. Diakses tanggal 05 Januari 2025
- Nugraheni, S. W., & Nurhayati, N. (2018). Aspek Hukum Rekam Medis Elektronik di RSUD Dr Moewardi. In *Prosiding Seminar Nasional Unimus* (Vol. 1).
- Qammaddin, Q. (2020). Keamanan Data Pembelajaran Online Jaringan Komputer Di Perguruan Tinggi. *Instruksional*, 2(1), 35-40.
- Rahmadiliyani, N., & Faizal, F. (2018). Kerahasiaan Rekam Medis Di Rumah Sakit Aveciena Medika Martapura. *Jurnal Manajemen Informasi Kesehatan Indonesia* , 6 (2), 69-78.
- Sofia, S., Ardianto, ET, Muna, N., & Sabran, S. (2022). Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Fasilitas Kesehatan. *Jurnal Rekam Medik & Manajemen Informasi Kesehatan* , 1 (2), 94-103.