Volume 3 Nomor 2 (2025) 79-91

The Journal of Management Information and Health Technology
e-ISSN: 3025 - 2962

# Analisis Aspek Keamanan Data Rekam Medis Dalam Implementasi Rekam Medis Elektronik di Rumah Sakit Umum Daerah Klungkung

Ni Kadek Mariani[1]

[1]*Department of Health Information Management, Klungkung General Hospital*
Jl. Flamboyan No.40, Semarapura Kauh, Kec. Klungkung, Kabupaten Klungkung

Corresponding author: Ni Kadek Mariani
Email: kadekmariani605@gmail.com

**ABSTRAK**

Perkembangan teknologi di dunia kesehatan telah berkembang pesat. Salah satu teknologi tersebut adalah penerapan sistem rekam medis elektronik. RSUD Kabupaten Klungkung merupakan salah satu rumah sakit yang telah menerapkan sistem rekam medis elektronik (RME) sejak tahun 2021. Dalam penerapannya terdapat beberapa kendala yang mengancam keamanan dan privasi rekam medis seperti kedisiplinan pegawai dan tidak terdapatnya SOP yang mengatur mekanisme keamanan *username* dan *password*. Potensi kebocoran atau kehilangan data merupakan ancaman serius dalam penerapan RME. Tujuan penelitian ini untuk menganalisis aspek keamanan data rekam medis pasien pada penerapan rekam medis elektronik di RSUD Kabupaten Klungkung, Metode penelitian menggunakan deskriptif kualitatif dengan teknik pengembilan sampel *Purposive sampling*. Sampel dalam penelitian ini berjumlah 9 orang. teknik pengumpulan data dengan cara wawacara. Hasil penelitian Implementasi RME di RSUD Kabupaten Klungkung menunjukkan keamanan informasi yang bervariasi. Privasi terancam oleh kelalaian pengguna, namun integritas dan autentikasi data telah terjamin melalui notifikasi otomatis, *username, password*, dan tanda tangan elektronik. Ketersediaan data penting untuk mutu layanan, didukung kontrol akses yang baik dan non-repudiasi melalui Tanda Tangan Elektronik. Optimalisasi sistem dan peningkatan kapasitas pengguna diperlukan. Secara kesluruhan pengelolaan aspek keamanan sistem RME di RSUD Kabupaten Klungkung cukup baik.
**Kata Kunci**: Aspek Keamanan; Rekam Medis Elektronik; Privasi dan Kerahasiaan.

***ABSTRACT***

*The development of technology in the world of health has grown rapidly. One of these technologies is the implementation of an electronic medical record system. Klungkung Regency Hospital is one of the hospitals that has implemented an electronic medical record system (EMR) since 2021. In its implementation, there are several obstacles that threaten the security and privacy of medical records such as employee discipline and the absence of SOPs that regulate the security mechanism of usernames and passwords. The potential for data leakage or loss is a serious threat in the implementation of EMR. The aim of this study was to analyze the security aspects of patient medical record data in the implementation of electronic medical records at the Klungkung Regency General Hospital. The research method uses qualitative descriptive with a purposive sampling technique. The sample in this study amounted to 9 people. Data collection techniques by interview. The results of the EMR Implementation study at Klungkung Regency Hospital show varying information security. Privacy is threatened by user negligence, but data integrity and authentication have been guaranteed through automatic notifications, usernames, passwords, and electronic signatures. Data availability is important for service quality, supported by good access control and non-repudiation through electronic signatures. System optimization and increasing user capacity are needed. Overall, the management of the security aspects of the RME system at Klungkung District Hospital is quite good.*
**Keywords:** *Security Aspects*; *Electronic Medical Records*; *Privacy and Confidentiality.*

## PENDAHULUAN

Dewasa ini pesatnya perkembangan teknologi dan sistem informasi memberikan pengaruh yang signifikan bagi penyedia layanan terhadap peningkatan kualitas pelayanan (Sofia, 2022). Salah satu perkembangan teknologi dibidang kesehatan adalah rekam medis elektronik (RME). RME merupakan repositori data pasien dalam bentuk digital, disimpan dengan aman, dapat diakses oleh banyak pengguna yang berwenang, berisi data retrospektif dan informasi prospektif untuk mendukung perawatan kesehatan terpadu, berkelanjutan, efisien dan berkualitas (Simanjuntak et al., 2022). Implementasi sistem RME secara signifikan membantu tenaga kesehatan dalam mendokumentasikan informasi secara lebih akurat dan terstruktur. Hal ini berkontribusi pada minimalisasi risiko kesalahan dalam pencatatan maupun interpretasi data (Andhani, 2023). Meskipun demikian, transformasi menuju sistem digital ini juga menghadirkan sejumlah tantangan dan risiko substansial. Potensi kebocoran atau kehilangan data merupakan ancaman serius yang harus diantisipasi dalam penerapannya.

Kasus kebocoran data pasien COVID-19 di Indonesia baru-baru ini menjadi perhatian publik setelah ditemukannya data berkapasitas 720 GB, yang berisi sekitar 6 juta informasi pasien, diperjualbelikan di forum daring oleh pengguna bernama Astarte. Data ini diduga berasal dari server Kementerian Kesehatan (Kemenkes) dan mencakup informasi sensitif seperti nama, foto, hasil tes COVID-19, hingga laporan radiologi (Rizkinaswara, 2022). Melihat insiden tersebut, tidak menutup kemungkinan akan terjadi pemalsuan data rekam medis elektronik. Pemalsuan ini dapat disebabkan oleh kelalaian tenaga kesehatan sendiri atau karena kebocoran data dalam sistem informasi rumah sakit.

Keamanan data dan informasi kesehatan merupakan prioritas utama yang harus diperhatikan. Berdasarkan standar SNI/ISO/IEC 27001, keamanan data sistem informasi mencakup kerahasiaan (*confidentiality*), keutuhan *(integrity*), dan ketersediaan (*availability*) (KEMENPU-PR. SPIP. No 4 Tahun, 2018) dan Sabarguna Tahun 2008 mengemukakan bahwa keamanan dalam sistem terkomputerisasi meliputi empat aspek utama: privasi, integritas, autentikasi, dan ketersediaan. Namun, dalam konteks sektor kesehatan, terdapat dua aspek tambahan yang krusial, yaitu kontrol akses (*access control*) dan nirpenyangkalan (*non-repudiation*) .

Privasi berfokus pada perlindungan informasi dari akses tidak sah, terutama untuk rekam medis yang merupakan dokumen rahasia pasien. Integritas memastikan bahwa data rekam medis elektronik tidak dapat dihapus atau diubah tanpa meninggalkan jejak, sehingga setiap modifikasi dapat dilacak. Autentikasi membatasi akses hanya kepada pihak yang berwenang, dengan mencatat identitas, waktu, dan tanda tangan petugas yang berinteraksi dengan sistem. Ketersediaan menjamin bahwa informasi dapat diakses dengan cepat oleh pihak terkait saat dibutuhkan. Akses kontrol melibatkan pengaturan teknis dan prosedural untuk mengelola siapa saja yang dapat mengakses informasi, sementara *Non-Repudation* memastikan bahwa individu tidak dapat menyangkal tindakan atau perubahan yang telah mereka lakukan terhadap informasi (Listyorini, 2021).

Keamanan data dan informasi rekam medis merupakan kewajiban fundamental yang harus dipatuhi oleh seluruh pihak terkait. Kewajiban ini diatur secara eksplisit dalam Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, yang secara tegas menyatakan bahwa tenaga kesehatan dan fasilitas pelayanan kesehatan memiliki tanggung jawab untuk menjaga keamanan dan kerahasiaan data pasien, termasuk rekam medis.

Lebih lanjut, Peraturan Menteri Komunikasi dan Informasi Nomor 4 Tahun 2016 Pasal 1 Ayat 5 tentang Penyelenggaraan Sistem Elektronik mewajibkan penyelenggara sistem elektronik untuk melaksanakan operasionalnya berbasis risiko. Dalam konteks ini, risiko didefinisikan sebagai potensi terjadinya kejadian atau kondisi yang tidak diinginkan, yang dapat menimbulkan dampak negatif signifikan terhadap kinerja dan kualitas layanan. Oleh karena itu, penerapan sistem rekam medis elektronik harus senantiasa mempertimbangkan dan mengelola risiko keamanan data secara komprehensif.

RSUD Kabupaten Klungkung, sebagai rumah sakit tipe B yang telah mengimplementasikan sistem rekam medis elektronik (RME) sejak tahun 2021, menghadapi beberapa tantangan terkait keamanan data. Observasi menunjukkan belum adanya Standar Operasional Prosedur (SOP) spesifik yang mengatur keamanan data rekam medis. Sejalan dengan hal tersebut, ditemukan kurangnya pemahaman di kalangan petugas kesehatan mengenai konsep privasi dan hak akses terhadap rekam medis. Ini mengindikasikan belum terbangunnya pemahaman komprehensif tentang pentingnya perlindungan dan keamanan data rekam medis elektronik pasien. Selain itu, sistem RME yang digunakan saat ini

belum dilengkapi fitur penggantian kata sandi secara berkala. Kondisi ini meningkatkan potensi kebocoran informasi yang dapat disalahgunakan oleh pihak tidak berwenang, serta berisiko tinggi terhadap pelanggaran privasi pasien.

Penelitian yang dilakukan oleh Ardianto Tahun 2024 menunjukan bahwa kurangnya fitur penggantian password secara berkala meningkatkan resiko penyalahgunaan kewenangan dan hak akses rekam medis (Ardianto & Nurjanah, 2024). Studi lain oleh Sofia Tahun 2022 menggarisbawahi bahwa dalam upaya menjaga keamanan rekam medis elektronik, sebuah sistem wajib memenuhi beberapa aspek krusial. Aspek-aspek tersebut meliputi kerahasiaan (melalui penggunaan nama pengguna dan kata sandi), autentikasi (melalui penerapan tanda tangan elektronik), ketersediaan, kontrol akses, dan nirsangkal (Sofia, 2022). Kedua penelitian ini mengindikasikan bahwa penerapan sistem RME memerlukan fitur keamanan, kebijakan dan beragam aspek dalam uapaya melindungi dari penyalahgunaan kerahasiaan informasi medis pasien.

Menjaga keamanan RME adalah imperatif mutlak. Perlindungan yang kokoh terhadap rekam medis tidak hanya esensial untuk mematuhi regulasi dan mencegah penyalahgunaan, tetapi yang terpenting adalah untuk menjamin privasi pasien serta integritas dan keberlangsungan pelayanan kesehatan yang berkualitas. Maka dari itu peneliti tertarik untuk melakukan penelitian bagaimana aspek keamanan data rekam medis pasien pada penerapan rekam medis elektronik di RSUD Kabupaten Klungkung

## METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah deskriptif dengan pendekatan kualitatif. Metode ini digunakan untuk menyelidiki, menemukan dan menggambarkan fenomena yang diteliti secara mendalam dan komprehensif mengenai aspek keamanan data dalam penerapan RME (Sahir, 2021).

Lokasi penelitian yaitu RSUD Kabupaten Klungkung dengan waktu penelitian maret 2025 sampai mei 2025. Populasi sampel dalam penelitian ini berjumlah 9 orang informan yang terdiri dari : 3 (Tiga) orang dari Manajemen RS, 3 (Tiga) orang dari Staf Rekam Medis dan 3 (Tiga) orang dari Staf SIMRS IT. Teknik pengambilan sampel menggunakan *Porposive Sampling,* teknik ini digunakan untuk mengambil sampel yang didasari atas penilaian mengenai siapa saja yang memenuhi syarat karakteristik dan ciri kriteria tertentu (Nasution, 2023). Kriteria yang dimaksud meliputi kriteria inklusi dan eksklusi.

Kriteria inklusi mencakup informan yang memiliki pengalaman pengoperasian RME selam 3 bulan dan aktif menggunakan RME dan berpartisipasi dalam penelitian dengan mengisi *informed consent.* Sedangkan kriteria eksklusi dalam penelitian ini meliputi informan sebagai pegawai baru dan tidak aktif menggunakan RME selama 3 bulan serta tidak bersedia menjadi informan penelitian ini. Penerapan kriteria ini bertujuan untuk memastikan bahwa informan yang terlibat memiliki karakteristik dan pemahaman yang memadai mengenai pengiperasian RME.

Jenis data yang dikumpulkan dalam penelitian ini adalah data primer dan data sekunder. Data primer dikumpulkan dengan cara wawancara menggunakan pedoman wawancara terstruktur yang diajukan dengan urutan dan formulasi yang sama untuk semua informan, memastikan standarisasi proses pengumpulan data (Nasution, 2023). Data sekunder dikumpulkan dengan observasi dan dokumensasi pada panduan, kebijakan dan standar prosedur operasional yang diterapkan di RSUD Kabupaten Klungkung berhubungan dengan aspek keamanan rekam medis elektronik.

Teknik Analisis data pada penelitian ini menggunakan Analisis tematik. Analisis tematik digunakan untuk menemukan pola dan tema utama terkait keamanan data dalam penerapan RME. Teknik ini mengacu pada metode (Braun & Clarke, 2006). Yang terdiri dari enam tahapan yaitu : (1) familiariasi dengan data,(2) generasi kode awal, (3) pendarian tema, (4) peninjauan tema, (5) definisi dan penamaan tema, (6) penyusunan laporan.

## HASIL DAN PEMBAHASAN

### Aspek Privacy Pada Penerapan Rekam Medis Elektronik di RSUD Kabupaten Klungkung

Peneliti mengidentifikasi jawaban informan dari 6 (enam) pertanyaan tentang *privacy* ke dalam 2 tema penelitian kualitatif yaitu pentingnya perlindungan data dan pelatihan terkait privasi RME dan kebijakan terkait perlindungan data pada sistem RME.

a. Perlindungan dan pelatihan terkait *Privasi* Data Rekam Medis Elektronik

Hasil wawancara dengan sembilan informan dari manajemen, staf rekam medis, dan staf IT di RSUD Kabupaten Klungkung secara konsisten menyatakan privasi data pasien sebagai komponen krusial dalam implementasi RME. Aspek privasi menjadi kewajiban hukum dalam menjaga

kerahasiaan rekam medis sebagaimana tertuang dalam Undang – Undang Nomor 17 Tahun 2023 tentang Kesehatan. Pasal 296 Ayat 5 setiap tenaga kesehatan dan fasilitas pelayanan mempunyai kewajiban menjaga kerahasiaan rekam medis. Dipertegas kembali Pasal 297 Ayat 3 fasilitas pelayanan kesehatan diharuskan menjaga keamaan, keutuhan, kerahasiaan dan ketersediaan data dan informasi yang terkandung dalam rekam medis.

Privasi, atau konfidensialitas, merupakan elemen vital untuk melindungi informasi kesehatan pasien dari akses atau penggunaan yang tidak sah (Soraya et al., 2025). Pentingnya privasi ini tidak hanya sebatas teori, melainkan juga tercermin dalam praktik layanan kesehatan dimana tenaga kesehatan dan fasilitas pelayanan kesehatan diwajibkan untuk menjaga kerahasiaan dan kepercayaan pasien terhadap rumah sakit(Meilia et al., 2019). Tidak semata memenuhi kewajiban melindungi privasi informasi medis saja. Akan tetapi, perlu disadari timbulnya ancaman yang krusial pasien pada penerapan RME. Salah satunya kesalahan pengguna.

Hasil penelitian menemukan beberapa kemungkinan ancaman terhadap aspek privasi di RSUD Kabupaten Klungkung seperti kelalaian dan keteledoran pengguna akan penggunaan kata sandi yang lemah, tidak terdapat perubahan kata sandi secara berkala. Kegagalan melakukan *logout* sistem sehingga akun pengguna masih terbuka pada sistem rekam medis. Serta masih adanya praktek pemberian akses kata sandi kepada petugas lain untuk membantu pengisian rekam medis. Ancaman teknis berupa serangan siber dan jaringan, kerentanan keamanan fisik karena tidak terdapat *finger print* di ruang penyimpanan rekam medis. Penelitian oleh Koemarinjanto Tahun 2023 mengenai keamanan loker penyimpanan bahwa keamanan dengan teknologi juga memberi masukan dimana penggunaan *fingerprint* dan *face recognition* terbukti berhasil memberikan kemanan dan menjaga privasi pengguna. Pengguna yang tidak mempunyai akses valid, maka ruang penyimpanan tidak akan terbuka (Koesmarijanto et al., 2023).

Kesalahan pengguna ini didasari atas ketidaktahuan akan pentingnya privasi yang digambarkan tidak adanya pelatihan khusus pengenai privasi. Hasil wawancara menunjukan tidak adanya pelatihan khusus mengenai privasi kepada petugas yang mengisi rekam medis. Pelatihan dilakukan hanya sebatas sosialisasi yang dilakukan oleh petugas yang belum pernah mendapatkan pelatihan privasi.

Kurangnya kesadaran akan risiko menjadi awal dari kegagalan dalam menjaga kerahasiaan informasi yang krusial. Kesadaran menjadi *point* sentral dari faktor pengguna yang menjadi kunci keberhasilan menjaga keamanan sistem informasi (Akraman et al., 2018). Penelitian oleh Purwawijaya Tahun 2025 mengenai kesadaran keamanan informasi menunjukan bahwa pengguna sistem informasi setalah diberikan pelatihan mengenai keamanan sistem informasi mengelami peningkatan pemahaman sebesar 66.6%. yang artinya terdapat perubahan prilaku kesadaran keamanan siber yang awalnya lalai menjadi lebih proaktif seperti penerapan dua faktor autentikasi dan mematuhi kebijakan yang berlaku (Purwawijaya et al., 2025).

Penelitian oleh Sari, dkk yang menunjukkan bahwa jaminan privasi merupakan fondasi utama dalam membangun kepercayaan antara pasien dan penyedia layanan kesehatan. Ketika pasien yakin bahwa informasi pribadi mereka akan dijaga kerahasiaannya, mereka cenderung lebih terbuka dan jujur dalam memberikan informasi kesehatan yang akurat dan lengkap. Hal ini sangat penting dalam proses perawatan pasien (Sari et al., 2021). Selanjutnya, Penelitian Kianti Tahun 2023 menemukan bahwa kepercayaan pengguna dipengaruhi oleh pengelolaan risiko dalam tantangan praktik penerapan sistem (Tiara & Kinanti, 2023).

Tanpa perlindungan yang memadai berupa keamanan sistem informasi, organisasi berisiko kehilangan aset informasi mereka (Bustami & Bahri, 2020). Sehingga dibutuhkan strategi dari organisasi sebagai penanganan ancaman dan manajemen resiko melalui pendidikan dan pelatihan. Hal tersbut bertujuan untuk membantu membangun sikap yang bertanggungjawab dan proaktif terhadap penggunaan teknologi digital (Syahputra et al., 2024).

b. Kebijakan dan Prosedur Perlindungan Data Pada Sistem Rekam Medis Elektronik

Hasil wawancara terkait kebijakan dan prosedur sistem rekam medis elektronik dan observasi pada lokasi penelitian, kebijakan yang dimaksud berupa panduan pelayanan RME dengan Nomor 838/14/RSUD/ 2022. Pada panduan tersebut telah diuraikan mengenai kewajiban dan otoritas kewenangan mengenai kerahasiaan untuk akses, tingkat akses, *editing*/ modifikasi dan menghapus segala informasi yang terdapat pada sistem RME. Proses tersebut terdokumentasi melalui metode rekam jejak atau *history log system*. Meskipun kebijakan mengenai privasi telah tertuang pada panduan, tetap diperlukan turunan regulasi terkait dari panduan tersebut berupa Standar Operasional Prosedur (SOP). Karena tidak ditemukan SOP yang mengatur akan privasi rekam medis elektronik.

SOP menjadi komponen penting yang dapat memastikan kepatuhan standar pelayanan untuk menciptakan kualitas pelayanan (Rahmawati et al., 2024).

Selain penerapan kebijakan strategi rumah sakit dalam menjaga keamanan dan melindungi kerahasiaan dengan cara penggembangan teknologi berupa *Role – Based Acces Control* (RBAC) atau kontrol akases berbasis peran. Metode ini diterapkan untuk membatasi hak akses seseorang hanya pada peran dan kewenangan mereka saja. Pengguna hanya bisa melihat, mengedit, atau menghapus data sesuai kewenangannya berdasarkan *ID* khusus pada setiap pengguna. RBAC kombinasi dari dua model kontrol akses yaitu *Mandatory Access Control (MAC)* dan *Discretionary Acces Control (DAC),* yang memungkinkan pengelolaan hak akses kepada sistem informasi lebih terstruktur dan efisien (Gemawaty & Yuliani, 2024).

Sejalan dengan hal tersebut, hasil penelitian oleh Rahman pada 2021 mengenai implementasi *Single Sign-On* dan *Role-Based Access Control* (RBAC) pada sistem informasi memberikan gambaran kemudahan dan keamanan pengguna untuk masuk ke dalam aplikasi dengan menggunakan *username* dan *password* (Rahman, 2021). Keamanan ini diperoleh dari pengaturan *role* dan memastikan tidak ada pengguna yang mampu mengakses data yang bukan hak nya dengan cara menembak *url* secara acak telah ditanggulangi dengan proses pengecekan pada halaman halaman tertentu. Pengguna yang tidak mempunyai akses valid, maka ruang penyimpanan tidak akan terbuka (Koesmarijanto et al., 2023).

RSUD Kabupaten Klungkung juga menerapkan sistem *loqout* otomatis. Sistem akan melakukan mengeluarkan akun apabila tidak terdapat *action* selama 30 menit pada sistem RME. Fungsi sistem *logout* digunakan apabila pengguna sistem telah selesai menggunakan aplikasi tersebut dan ingin keluar dari aplikasi tersbut dengan mengklik tombol logout (Madhrozji & Effiyaldi, 2019). Hal ini diterapkan untuk memastikan tidak adanya akses *illegal* yang disebabkan oleh masih terbukanya *ID* atau *username* dan *password* dari pengguna yang belum melakukan *logout* pada saat selesai menggunakan sistem RME.

Implementasi berbagai strategi untuk melindungi dan menjaga kerahasiaan informasi kesehatan pasien dalam penerapan RME tetapi adopsi teknologi keamanan yang lebih mutakhir atau baru tetap menjadi suatu keharusan. Selain itu, kolaborasi interdisipliner antar unit terkait mencakup manajemen, rekam medis, dan teknologi informasi guna merumuskan strategi keamanan serta mekanisme pengawasan yang lebih komprehensif dan terintegrasi

**Aspek *Integrity* Pada Penerapan Rekam Medis Elektronik di RSUD Kabupaten Klungkung**

a. Integritas Data, Validitas dan Audit Sistem Rekam Medis Elektronik

Hasil wawancara menunjukan pemahaman seragam mengenai integritas, validitas dan audit data dalam sistem rekam medis yang komprehensif. RSUD Kabupaten Klungkung telah memiliki sistem audit berkala yang terprogram pada instalasi rekam medis dan medikolegal. SOP yang ada mengindikasikan audit kelengkapan pengisian rekam medis ebagai salah satu kegiatan yang menjamin integritas. Selain itu, keberadaan Komite Rekam Medis secara struktural mempunyak tugas menjamin integritas data dalam kegiatannya melaksankan review rekam medis meliputi indetifikasi, autentikasi, pencatatan dan pelaporan.

Penerapan standar meta data yang mengacu pada Keputusan Menteri Kesehatan Nomor HK.01.07/MENKES/1432/2022 tentang Pedoman Variabel dan Meta Data Pada Penyelenggaraan Rekam Medis Elektronik dan Penerapan Master dat ICD (*International Classification of Diseases*) menambah proses validitas data secara otomatis sehingga integritas data rekam medis dapat dijamin. Proses tersebut memberikan jaminan efektivitas kerja dan meningkatkan integritas data antara sitem manajemen rumah sakit dengan sistem lainnya (Aulia & Sari, 2023).

Sistem RME secara *flowchat* serta otomatis menyediakan notifikasi atau konfirmasi kepada pengguna sebelum data disimpan secara permanen. Mekanisme ini bertujuan untuk memastikan keakuratan data dan memberikan kesempatan kepada pengguna untuk meninjau kembali informasi yang diinput sebelum terekam dalam sistem. Integritas data merupakan jaminan terhadap keakuratan data dan informasi yang ada di dalam rekam medis elektronik (Ardianto & Nurjanah, 2024). Sistem RME yang ada saat ini dinilai telah memiliki berbagai fitur untuk menjaga integritas data secara proaktif

b. Pencegahan Modifikasi Data dan Pemulihan Data Rekam Medis Elektronik

Mekanisme pencegahan modifikasi data dan pemulihan data RME adalah hal penting bagi keberlangsungan sistem. Untuk mencegah kesalahan input, sistem dapat dilengkapi fitur notifikasi atau konfirmasi sebelum data disimpan secara permanen. Penelitian menunjukkan bahwa sistem RME

mengimplementasikan status dokumen *"draf*" dan "*final*" pada setiap formulir rekam medis. Seperti yang diungkapkan hasil wawancara di atar, "...beberapa *field* form di-set menjadi *Read-Only*, dan di setiap form rekam medis sudah dilengkapi dengan status dokumen *'draf*' dan *'final*'. pihak yang berwenang yang dapat mengubah data tertentu dan biasanya setiap form rekam medis sudah dilengkapi dengan status dokumen '*draf*' dan '*final*'."

Penggunaan status "*draf*" memungkinkan perubahan data, sementara status "*final*" menandakan bahwa dokumen telah terkunci. Setelah suatu dokumen dinyatakan final, data di dalamnya tidak dapat diubah secara sembarangan. Selain itu, beberapa kolom dapat diatur menjadi mode *read-only* untuk mencegah modifikasi yang tidak sah. Mekanisme ini menjamin integritas dan otentisitas data medis yang tersimpan dalam sistem. Integritas dalam RME berarti data yang tersimpan dalam sistem harus akurat, konsisten, dan utuh. Informasi yang ada harus sesuai dengan kenyataan, tidak dimanipulasi, serta mematuhi standar yang berlaku

Upaya pencegahan modifikasi yang tidak sah berfokus pada penerapan prinsip keamanan informasi seperti privasi, integritas, autentikasi, ketersediaan, kontrol akses, dan non-repudiasi. Implementasi Sistem Informasi Manajemen Rumah Sakit (SIMRS) juga menjadi bagian dari upaya ini. Selain itu, rumah sakit dapat menerapkan doktrin tanggung jawab berdasarkan kesalahan *(vicarious liability)* untuk mengelola risiko hukum terkait kebocoran data (Budiman et al., 2025).

Hasil penelitian secara komprehensif menunjukkan bahwa integritas data dalam sistem RME terjamin melalui implementasi strategi pencadangan (*backup*) data yang terstruktur dan berlapis. Secara konsisten menyatakan bahwa pemulihan data dilakukan melalui proses *restore* dari hasil *backup* yang dilaksanakan secara berkala. Hal ini mengindikasikan adanya prosedur standar operasional untuk menghadapi potensi kehilangan data. Pencadangan data dilakukan setiap minggu dan memanfaatkan berbagai media penyimpanan, termasuk *cloud storage* dan *Network Attached Storage* (NAS) untuk pencadangan lokal. Penggunaan kombinasi *cloud* dan penyimpanan lokal menunjukkan pendekatan yang kokoh dalam menjaga ketersediaan dan redundansi data.

Melihat analisis tersebut maka dapat disimpulkan bahwa sistem RME ini memiliki mekanisme mitigasi risiko kehilangan data yang efektif dan terencana. Strategi pencadangan yang terstruktur, periodik, dan didukung oleh beragam media penyimpanan ini memastikan kontinuitas layanan dan integritas data rekam medis pasien, yang merupakan aspek krusial dalam pelayanan kesehatan digital.

**Aspek *Authentication* Pada Penerapan Rekam Medis Elektronik di RSUD Kabupaten Klungkung**

a. Kebijakan Identifikasi dan Autentikasi Sistem Rekam Medis Elektronik

Prosedur atau kebijakan terkait identifkasi dan autentifikasi pengguna rekam medis elektronik merupakan bagian penting dari menjaga kerahasiaan rekam medis dari akses yang tidak sah. metode autentikasi yang digunakan pada implementasi RME di RSUD Kabupaten Klungkung yaitu penerapan *username* dan *password.* Kata sandi yang digunakan adalah kombinasi huruf, angka, dan simbol untuk meningkatkan kekuatan. Seluruh informan menyatakan bahwa setiap pengguna memiliki *username* dan *password* yang unik dan dibatasi hak aksesnya sesuai dengan peran *(Role Based Access Control).*

Keamanan proses login meskipun dianggap cukup aman dengan adanya *username* dan *password* unik serta pembatasan hak akses, 7 (tujuh) informan menganggap keamanan ini belum optimal. Belum adanya *Two-Factor Authentication* (2FA) seperti biometrik (sidik jari/pengenalan wajah) atau OTP (*One-Time Password*) melalui *whatsApp/email* menjadi perhatian utama. Implementasi biometrik baru terbatas pada sistem pendaftaran, kekhawatiran muncul mengenai potensi akses oleh pihak tidak bertanggung jawab jika mengetahui *username* dan *password* pengguna

Selain penerapan *username* dan *password* sebagai identifikasi identitas. Dari autentikasi juga telah menerapkan tanda tangan elektronik pada setiap dokumen yang akan disi berdasarkan *username* dan *password* login pada sistem. Manajemen identifikasi dan autentikasi khususnya tanda tangan elektronik tersertifikasi belum dibahasakan dalam regulasi rumah sakit, Proses pengusulan kebijakan ini terhambat oleh birokrasi yang panjang dan kendala anggaran. Meskipun demikian, evaluasi terhadap penerapan TTE sudah dilakukan, dan komunikasi berkala dengan Dinas Komunikasi dan Informatika (Kominfo) Kabupaten Klungkung.

Mengatasi kendala tersebut berdasarkan observasi dan dokumentasi manajemen telah menerapkan kebijakan mengenai penggunaan tanda tangan elektronik non sertifikasi. Hal ini secara spesifik diatur dalam Surat Keputusan Direktur Nomor 139 Tahun 2021 tentang Pemberlakuan Tanda Tangan Elektronik pada Rekam Medis

Elektronik di RSUD Kabupaten Klungkung. Pemberlakuan Surat Keputusan ini mengindikasikan bahwa RSUD Kabupaten Klungkung telah memiliki kebijakan formal terkait penerapan autentikasi berbasis tanda tangan elektronik untuk sistem RME mereka.

Penelitian yang dilakukan oleh Lestari Tahun 2025 dalam aspek autentikasi, Rumah Sakit Kartini telah menerapkan tanda tangan digital berupa *barcode*, dan setiap karyawan memiliki akun individual. Terkait integritas data, sistem rekam medis elektronik di Rumah Sakit Kartini memastikan bahwa tidak semua karyawan dapat mengubah atau mengedit konten. Hal ini dicapai melalui hak akses yang berbeda-beda untuk setiap pengguna. Selain itu, perubahan data tidak menghilangkan informasi sebelumnya, melainkan ditandai dengan garis merah sebagai indikasi modifikasi (Santi Lestari & Azizah, 2025).

RSUD Kabupaten Klungkung perlu melihat penerapan pada penelitian terdahulu serta peraturan yang mengatur mengenai sertifikat elektronik atau tanda tangan elektronik pada sistem informasi. Guna meningkatkan identifikasi dan autentifikasi dalam kapasitas peningkatan sistem RME. Penerapan rekam medis elektronik membutuhkan kapasitas identifikasi dan autentikasi yang kuat untuk memastikan keamanan dan keabsahan data pasien. Identifikasi dan autentikasi dalam RME berfungsi untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sistem dan data yang tersimpan di dalamnya.

b. Autentifikasi Sistem dan Evaluasi Sistem Autentifikasi Rekam Medis Elektronik

Menerapkan autentifkasi dan evaluasi sistem pada rekam medis elektronik, maka kerahasiaan data pada rekam medis elektronik dapat terjaga dengan baik. Berdasarkan hasil analisis wawancara tersebut dapat digambarkan pengelolaan kata sandi di RSUD Kabupaten Klungkung memungkinkan pengguna untuk melakukan reset kata sandi secara mandiri. Administrator juga memiliki kemampuan untuk mengelola kata sandi pengguna. Ada prosedur standar pemberian kata sandi awal dan kemudian mengarahkan pengguna untuk menggantinya. Audit Trail dan evaluasi berkala telah dilakukan, sistem sudah memiliki audit trail yang mencatat setiap akses pengguna, termasuk siapa, kapan, dan apa yang dilakukan. Evaluasi berkala terhadap kekuatan sistem autentikasi secara khusus masih belum ada secara komprehensif, namun masalah atau kendala yang muncul biasanya langsung ditindaklanjuti oleh tim IT dan rekam medis.

Evaluasi terkait tanda tangan elektronik dilakukan setiap 3 bulan sekali melalui komunikasi dengan Kominfo. Masalah yang muncul dari jawaban informan sejauh ini tidak ada hal yang signifikan terkait proses autentikasi (login langsung berhasil jika *username* dan *password* sesuai).

Penelitian serupa oleh Destri Maya Rani pada RSI Sultan Agung mengemukakan bahwa melalui kemampuan sistem dalam mencatat setiap jejak perubahan data, baik berupa penambahan maupun modifikasi yang dilakukan oleh pengguna. Setiap aktivitas yang terjadi dalam sistem secara otomatis direkam dan disimpan, sehingga tidak ada perubahan yang bisa dimanipulasi atau dihapus tanpa tercatat. Catatan ini berfungsi sebagai bukti audit dan hanya dapat diakses oleh tim IT yang berwenang, yang bertanggung jawab untuk memantau dan menjaga integritas data. Setiap tindakan, termasuk akses, perubahan, atau penghapusan data, dapat dilacak secara rinci, memastikan bahwa semua aktivitas tercatat dengan baik dan dapat ditinjau jika diperlukan (Rani & Widyaningrum, 2025)

Setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggungjawab terhadap beroperasinya sistem elektronik sebagaimana mestinya. Penggunaan tanda tangan digital dalam transaksi rekam medis elektronik berfungsi sebagai alat untuk autentikasi dan verifikasi atas identitas penandatanganan serta keutuhan dan keautentikan informasi elektronik. Penggunaan tanda tangan digital (*digital signature*) berfungsi sebagai alat untuk autentikasi dan verifikasi atas identitas penandatangan serta keutuhan dan keautentikan informasi elektronik. Tujuan penggunaan tanda tangan digital pada rekam medis elektronik adalah untuk memberikan autentifikasi dan penjagaan atas privasi terhadap isi atau data medis tiap-tiap pasien yang dibubuhkan pada akhir dokumen sebelum dokumen tersebut disimpan dalam sebuah sistem informasi manajemen rumah sakit (SIMRS-EMR) secara elektronik. Tanda tangan digital menjadi kunci utama dari aspek ini. Tanpa tanda tangan digital, rekam medis elektronik akan menjadi lubang dari privasi data pasien yang seharusnya dilindungi sepenuhnya oleh pihak rumah sakit (Fitriyah, 2022).

Merujuk pada rangkuman penelitian dan hasil penelitian terdahulu, menjadi krusial untuk RSUD Kabupaten Klungkung lebih meningkatkan komunikasi terkait penyusunan kebijakan dan prosedur identifikasi, autentifikasi serta pencanangan TTE untuk mewujudkan integritas rekam medis elektronik terintegrasi yang legal tidak hanya dari sisi dokumen tetapi juga perlindungan

sumber daya kesehatan yang menerapkan RME dalam pelayanan kesehatan.

**Aspek *Availability* Pada Penerapan Rekam Medis Elektronik di RSUD Kabupaten Klungkung**

a. Ketersediaan Sistem dan Sumber Daya Rekam Medis Elektronik

Berdasarkan pada bahasan wawancara tersebut dapat dijabarkan bahwa RSUD Kabupaten Klungkung berkomitmen untuk mengembangkan rekam medis elektronik sesuai kebutuhan *user* (pengguna). Informan memahami pentingnya ketersediaan data dan informasi rekam medis dalam mendukung mutu layanan, kepuaasan dan keselamatan pasien. Seluruh informan memahami kebutuhan sumber daya dalam mengembangkan sistem dan peningkatan kapasitas layanan termasuk dalam pendidikan dan pelatihan.

Penjelasan pasal 29 Permeneks RI Nomor 24 Tahun 2022 menyiratkan 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. Nilai guna rekam medis dalam hal alat komunikasi, maka rekam medis baiknya dapat diakses dengan cepat dan dapat menampilkan kembali data yang telah tersimpan.

Pengaturan Rekam Medis bertujuan untuk: a. meningkatkan mutu pelayanan kesehatan; b. memberikan kepastian hukum dalam penyelenggaraan dan pengelolaan Rekam Medis; c. menjamin keamanan, kerahasiaan, keutuhan, dan ketersediaan data Rekam Medis; dan d. mewujudkan penyelenggaraan dan pengelolaan Rekam Medis yang berbasis digital dan terintegrasi. Sebagaimana penelitisn oleh Riska Pradita tentang penerapan RME di Puskesmas yang menyebutkan mewujudkan penyelenggaraan sistem informasi Puskesmas yang terintegrasi, menjamin ketersediaan data dan informasi yang berkualitas, berkesinambungan, dan mudah diakses, serta meningkatkan kualitas pembangunan kesehatan di wilayah kerjanya melalui penguatan manajemen Puskesmas (Pradita et al., 2022)

Aspek *availability* dalam penelitian juga diteliti oleh Untung Slamet Suhariyono pada Puskesmas Karangploso yang menemukan bahwa pentingya ketersediaan daya internet yang sangat tinggi, sehingga saat membutuhkan data pasien dapat diakses dengan cepat. Puskesmas telah bekerjasama dengan dinas kesehatan dan menggunakna aplikasi E-Puskesmas, sehingga penyimpanan data dilakukan melalui database. Data akan tersimpan secara otomatis, sehingga tidak ada risiko kehilangan selama 25 tahun (Suhariyono et al., 2025)

b. Prosedur Penanganan *Downtime* dan Strategi *Back up* Data Rekam Medis Elektronik

Prosedur penanganan *downtime* dan strategi *backup* data rekam medis elektronik penting untuk memastikan kontinuitas layanan dan keamanan data. *Downtime* RME dapat terjadi karena berbagai alasan, dan penanganan yang tepat serta *backup* data yang terjadwal akan sangat membantu dalam meminimalkan dampak yang ditimbulkan akibat *downtime.*

Melihat hasil wawancara mengenai penanganan *downtime* dan *backup* data maka penting pemahaman prosedur dan penerapan langkah dalam mengatasi *downtime* dipahami oleh seluruh unit pengguna RME di RSUD Kabupaten Klungkung. Data *backup* dan *recovery* merupakan proses untuk membuat salinan data sebagai upaya mencegah kehilangan dan menyiapkan sistem yang aman sehingga nantinya data bisa kembali dipulihkan. Data *backup* memerlukan *copy* dan pengarsipan data komputer agar dapat diakses jika terjadi kerusakan atau data dihapus. *Backup* secara teratur dan konsisten agar meminimalkan data yang hilang. Semakin banyak waktu yang dihabiskan untuk *backup* secara rutin, maka semakin besar kemungkinan Anda untuk memulihkan kembali ketika data itu dibutuhkan (Anggraini, 2023).

Langkah tersebut dibahas juga dalam Standar akreditasi MRMIK 13.1 dimana pemenuhan standar untuk rumah sakit agar dapat mengembangkan, memelihara, dan menguji program untuk mengatasi waktu henti (*downtime* dari sistem data, baik secara terencana maupun tidak terencana. Sistem data adalah bagian yang penting dalam memberikan perawatan/pelayanan pasien yang aman dan bermutu tinggi. Interupsi dan kegagalan sistem data adalah kejadian yang tidak bisa dihindari.: a) Terdapat prosedur yang harus dilakukan jika terjadi waktu henti sistem data *(dowtime)* untuk mengatasi masalah pelayanan. b) Staf dilatih dan memahami perannya di dalam prosedur penanganan waktu henti sistem data *(downtime),* baik yang terencana maupun yang tidak terencana. c) Rumah Sakit melakukan evaluasi pasca terjadinya waktu henti sistem data *(down time)* dan menggunakan informasi dari data tersebut untuk persiapan dan perbaikan apabila terjadi waktu henti *(downtime)* berikutnya (Abiyyu & Annisa, 2024).

Langkah tersebut dibahas juga dalam penelitian tentang *downtime* dan *backup* data RME

di RSUD Cilacap, bahwa pengawasan dalam pengisian rekam medis elektronik sudah sesuai prosedur. Kendala yang dihadapi saat pengisian berkas rekam medis yaitu *downtime* sistem, *error* sistem sering terjadi, isian data kadang hilang sendiri, dan gangguan sistem atau *server*. Cara mengatasi hambatan-hambatan tersebut yaitu menunggu selama 30 menit untuk mengetahui sistem kembali normal. Jika setelah 30 menit sistem masih bermasalah,maka dilakukan pendaftaran manual, jika gangguan berlanjut menghubungi vendor atau IT RS (Nurhadiulhaq & Wulandari, 2025).

RSUD Kabupaten Klungkung telah meanjalankan prosedur dan langkah dalam mengatasi hambatan dan dampak *downtime* dengan sistem *back up* data yang dilakukan sesuai jadwal *update* sistem sebagaimana hasil wawancara tersebut diatas. Pemahaman kebijakan dan prosedur adalah langkah awal ketersediaan data ketika dibutuhkan. Semua pihak terkait perlu pemahaman lebih mendalam bahwa ketersediaan data tidak hanya untuk internal rumah sakit tetapi juga eksternal seperti, kebutuhan akreditasi sesuai standar MRMIK Starkes 2024 yang dapat dikembangkan dalam pedoman dan prosedur rekam medis elektronik di rumah sakit.

**Aspek *Acces Control* Pada Penerapan Rekam Medis Elektronik di RSUD Kabupaten Klungkung**

a. Hak Akses Sesusi Peran dan Tanggung Jawab Pengguna

RSUD Kabupaten Klungkung telah menjalankan sistem review dalam pengelolaan akses kontrol pengguna RME. Peran dan tanggung jawab dari masing – masing user (pengguna) telah ditetapkan dengan SK Direktur melalui pedoman rekam medis elektronik.

Keputusan Direktur Nomor 838/14/2022 Tentang Pedomen Pelayanan Rekam Medis ditetapkan 3 (tiga) katagori akses kontrol dalam RME di RSUD Kabupaten Klungkung meliputi hak akses sebagai penginput, perbaikan dan melihat data. (1) Hak akses penginputan merupakan memberikan hak akses kepada tenaga kesehatan yang memiliki wewenang dan tanggung jawab sebagai petugas pemberi pelayanan, (2) hak akses perbaikan data merupakan hak akses kepada tenaga yang telah memiliki akses penginputan akan tetapi hanya pada data yang menjadi tanggungjawabnya, dan (3) hak akses melihat (*read only)* pemberian hak akses kepada tenaga kesehatan yang telah memiliki username dan password kedalam sistem RME tapi tidak dapat melakukan perubahan atau penginputan data. Pemberian hak akses tersebut sepenuhnya menjadi kewenangan pimpinan rumah sakit. Pengaturan ini bertujuan untuk membatasi akses setiap individu terhadap rekam medis berdasarkan kewenangan dan lingkup tanggung jawab mereka.

Rekam Medis Elektronik merupakan salah satu produk perkembangan teknologi informasi yang dimaksudkan untuk mempermudah pelayanan kesehatan. Pemanfaatan sistem rekam medis elektronik tentu harus disempurnakan dengan pengamanan dan perlindungan data, termasuk kerahasiaan, autentikasi, dan *access control.* Aspek *access control* adalah upaya penjagaan informasi dari pengaturan akses pengguna ke sistem informasi. Penelitian tentang gambaran aspek *access control* pada RME pernah dilakukan oleh Nadilla Putri Melisa pada RSUD dr. Soediran Mangun Sumarso dimana diperoleh keamanan data pasien pada aspek *access control* tidak sesuai karena belum ada SPO tentang kebijakan maupun prosedur pengoperasian sistem rekam medis elektronik (Melisa et al., 2024).

Aspek *acces control* adalah aspek yang berhubungan dengan pengaturan akses pengguna kepada suatu sistem informasi. Proses *access control* digunakan untuk memastikan bahwa hanya orang-orang yang berwenang dan punya alasan yang absah, terkait dengan pengoperasian sistem informasi kesehatan. *Access control* dapat mengatur siapa-siapa saja yang berhak untuk mengakses infomasi atau siapa-siapa saja yang tidak berhak mengakses informasi. Hal ini dimaksudkan agar keamanan data pasien didalamnya dapat terjamin. Hal tersebut diungkapkan dalam penelitian oleh Siti Sofia, dkk dimana diperoleh bahwa pada dasarnya, fasilitas kesehatan telah menerapkan aspek *access control* pada rekam medik elektroniknya dengan melakukan pembatasan hak akses, namun masih ada beberapa fasilitas kesehatan yang belum maksimal dalam menerapkan pembatasan hak akses. Hal tersebut dapat dapat menimbulkan risiko kebocoran karena terbukanya data oleh pihak yang tidak memiliki wewenang dalam mengakses informasi tersebut (Sofia et al., 2022).

b. Penetapan Pengelolaan Hak Akses dan *Review* Hak Akses Penguna Rekam Medis Elektronik

Penetapan pengelolaan hak akses dan *review* hak akses pengguna rekam medis elektronik adalah proses penting untuk memastikan keamanan dan kerahasiaan data pasien. Hal ini diatur dalam peraturan perundang-undangan, khususnya Peraturan Menteri Kesehatan (PMK) Nomor 24 Tahun 2022 tentang Rekam Medis Elektronik. Berdasarkan hasil rekapan wawancara tersebut

dapat dipandang bahwa sistem yang diberlakukan RSUD Kabupaten Klungkung dalam pemenuhan aspek pengelolaan hak akses dan *review* hak akses sudah dijalankan dengan baik. Melihat dokumentasi dan observasi lanjutan, peneliti belum melihat hasil *review* dibuat dalam sistematika laporan sesuai tata naskah rumah sakit dan dilaporkan kepada pimpinan rumah sakit dalam hal ini Direktur sebagai penanggungjawab utama dalam penyelenggaraan RME pada tahun berjalan peneltiian di 2025. Menindaklanjuti hal tersebut, diperoleh informasi dari Instalasi Rekam Medis dan Medikolegal bahwa terkahir laporan dibuat pada tahun 2024, maka sesuai pedoman rumah sakit, review baiknya dilakukan setiap 3 bulan sekali sesuai tugas dan tanggung jawab komite rekam medis RSUD Kabupaten Klungkung.

Penelitian oleh Destri Maya Rani dalam penerapan keamanan sistem informasi di RSI Sultan Agung juga menemukan pembatasan akses RME dengan *ID* dan *password*. Hanya petugas rekam medis yang mempunyai hak akses terbatas yang dapat mengakses data pasien. Hanya pengguna yang berwenang yang dapat melihat dan mengelola informasi medis pasien. Akses internet bagi petugas rekam medis juga dibatasi untuk mencegah akses tidak sah atau penyalahgunaan informasi pasien melalui jaringan internet (Rani & Widyaningrum, 2025).

Penelitian yang dilakukan di Rumah Sakit Avicean Medika Martapura menunjukkan bahwa pada rumah sakit tersebut belum ada aturan secara resmi yang menerapkan siapa saja yang dapat mengakses rekam medis elektronik tersebut, tetapi sudah terdapat draf-draf yang berhak dan berwenang dalam hak akses rekam medis elektronik namun belum disahkan secara resmi. Rekam medik elektronik hanya dapat diakses oleh pengguna tertentu. Jika ada pasien yang membutuhkan resume medis maka pasien harus mengisi surat permintaan terlebih dahulu. Prosedur ini melindungi rekam medis elektronik dari petugas yang tidak berwenang. Hak akses catatan pengguna dapat diberikan secara terperinci kepada perusahan atas seijin pengguna. Penyelenggara sistem elektronik wajib melaksanakan prinsip pelindungan data pribadi dalam melakukan pemrosesan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepengetahuan dan persetujuan dari pemilik data pribadi (Sofia et al., 2022).

RSUD Kabupaten Klungkung telah menerapkan prinsip akses control, membatasi hak akses dan mereview pengguna akses. Hal tersebut telah ditetapkan dalam pedoman dan panduan kerja komite rekam medis, tetapi dalam hal *review* tersebut dibuat dalam sistematika pelaporan sesuai tata naskah rumah sakit belum terpenuhi. Proses pengelolaan hak akses akan menjadi lebih baik ketika pimpinan fasilitas pelayanan kesehatan lebih aware dan memberi perhatian lebih tidak hanya untuk kontrol internal tetapi juga sebagai pemenuhan standar akreditasi rumah sakit dalam hal menjaga mutu dan integritas data RME.

**Aspek *Non – Repudation* Pada Penerapan Rekam Medis Elektronik di RSUD Kabupaten Klungkung**

a. Pemantauan dan Pencatatan Aktivitas Pengguna Rekam Medis Elektronik

Berdasarkan hasil wawancara diketahui bahwa seluruh informan dapat memeberikan gambaran bagaimana sistem mencatat mulai dari identitas, waktu dan jenis aktivitas yang dilakukan *user* (pengguna) rekam medis elektronik di RSUD Kabupaten Klungkung. Hal tersebut meski sudah berjalan baik dan diketahui oleh informan, tetapi masih terdapat satu informan yang menyatakan kemungkinan penggunaan *user* dan *password* oleh yang tidak ber hak atas itu ada terjadi, contoh yang diberikan oleh informan adalah profesi dokter.

*Non-repudiation* menghalangi pengguna untuk menyangkal keterlibatan mereka dalam transaksi atau perubahan data dalam sistem. Ancaman keamanan informasi mencakup ketidaktahuan dan kecerobohan karyawan, seperti berbagi sandi atau menangani data secara tidak aman, serta serangan eksternal seperti virus, *spyware,* dan upaya peretasan. Sebagaimana penelitian yang dilakukan oleh Arif Budiman, dkk di RS P Surakarta, dimana menerapkan prinsip *non-repudiation* dengan mencatat dan melacak semua transaksi dan modifikasi data melalui *log audit*. Sistem RME secara otomatis mencatat perubahan data dan menyediakan pemberitahuan atas aktivitas pengguna, mencegah akses ilegal atau manipulasi data (Budiman et al., 2025).

Penyelenggara Sistem Elektronik wajib menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan Sistem Elektronik. Rekam jejak audit sebagaimana dimaksud digunakan untuk keperluan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, pengujian, dan pemeriksaan lainnya. Penelitian oleh Siti Sofia, dkk menghasilkan informasi bahwa memenuhi aspek *non repudiation* maka setiap tindakan yang dilakukan dalam sebuah sistem yang aman harus diawasi *(logged)*, ini dapat berarti penggunaan alat untuk melakukan pengecekan sistem berfungsi sebagaimana seharusnya. Fitur riwayat transaksi juga tidak dapat dipisahkan dari bagian keamanan sistem yang dimana bila terjadi

sebuah penyusupan atau serangan lain akan sangat membantu proses investigasi. Pemilihan jenis metode transmisi juga mempunyai peranan penting didalam masalah keamanan. Setiap informasi rahasia tidak boleh di transmisikan tanpa menggunakan enkripsi yang bagus, sehingga setiap orang dapat menyadap komunikasi yang terkirim. Aspek ini sangat penting dalam hal transaksi elektronik. Penggunaan *digital signature* dan teknologi kriptografi secara umum dapat menjaga aspek ini. Akan tetapi hal ini masih harus didukung oleh hukum sehingga status dari digital signature itu jelas legal (Sofia et al., 2022).

RSUD Kabupaten Klungkung telah menerapkan TTE (Tanda Tangan Elektronik) sebagai bagian dari pemenuhan aspek *non-repudiation* dalam pengisian rekam medis. Evaluasi yang perlu dilakukan adalah penggunaan *user* dan *password* oleh yang tidak berhak, jadi ketika ada kasus baik internal maupun eksternal tidak menambah beban rumah sakit dalam menentukan pertanggungjawaban keamanan data dan informasi RME.

b. Kebijakan terkait *non Repudation* dan Validitas Bukti Digital

RSUD Kabupaten Klungkung menerapkan kebijakan dengan pedoman dan petunjuk teknis terkait log aktivitas untuk memantau perubahan yang dilakukan dalam pengisian rekam medis elektronik. Monitoring dan evaluasi dilakukan secara berkala sesuai waktu rapat yaitu 3 (tiga) bulan sekali. *Non-repudiation* dalam konteks bukti digital menjamin bahwa pihak yang terlibat dalam transaksi atau komunikasi tidak dapat menyangkal tindakan digital mereka, seperti tanda tangan digital atau pengiriman pesan. UU ITE dan KUHAP mengakui bukti digital sebagai sah jika memenuhi syarat autentikasi dan relevansi.

Jenis bukti digital yang relevan dalam kasus seperti ini termasuk catatan log server, catatan aktivitas akun, pesan digital, dan metadata. Catatan *log server* dapat menunjukkan *IP address* dan t*imestamp* dari aktivitas yang mencurigakan, sedangkan catatan aktivitas akun dapat menunjukkan detail waktu dan isi dari aktivitas akun tersebut. Sebagaimana penelitian oleh Nurrachma Maharani, dkk adapun terkait validitas bukti digital dalam proses hukum Indonesia diatur oleh Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Kitab Undang-Undang Hukum Acara Pidana (KUHAP). UU ITE secara khusus mengakui bukti elektronik sebagai alat bukti yang sah, asalkan memenuhi kriteria autentikasi dan relevansi. Proses autentikasi ini sangat kritis, melibatkan verifikasi bahwa data belum diubah atau dimanipulasi sejak pengumpulan (Maharani et al., 2024).

Sebagai sebuah konsep dalam keamanan informasi, *non-repudiation* dirancang untuk mencegah pihak yang terlibat dalam transaksi digital dari menyangkal atau menolak keterlibatannya di masa mendatang. Mekanisme kerja *non-repudiation* mencakup beberapa langkah utama, seperti identifikasi, autentikasi, dan penggunaan tanda tangan digital serta sertifikat digital yang dikeluarkan oleh otoritas terpercaya. Selain itu, pencatatan *log* dan jejak audit memastikan akuntabilitas dalam setiap tahap transaksi. Tantangan yang dihadapi termasuk pengelolaan kunci kriptografi, kesesuaian regulasi, interoperabilitas sistem, serta biaya implementasi yang mungkin tinggi (Muhammad Bachtiar Nur Fa' Izi, 2024).

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik memberikan panduan lebih rinci tentang standar keamanan yang harus dipenuhi oleh penyelenggara sistem elektronik, termasuk dalam sektor hukum. Regulasi ini mencakup aspek kerahasiaan, integritas, ketersediaan, keaslian, dan kenirsangkalan (*non-repudiation*) data elektronik. Hal tersebut juga diungkapkan dalam penelitian yang dilakukan oleh Moody Rizqy Syailendra Putra, dkk yang menyatakan dua prinsip lain yang relevan dalam konteks hukum Indonesia: 1. autentikasi (*Authentication*): Memverifikasi identitas pengguna yang mengakses data hukum untuk mencegah akses tidak sah. 2. Nir-sangkal (*Non-repudiation*): Memastikan bahwa pihak yang terlibat dalam transaksi atau komunikasi elektronik tidak dapat menyangkal keterlibatan mereka Pelaksanaan audit keamanan dan evaluasi sistem secara berkala dapat membantu mengidentifikasi kelemahan dan meningkatkan keamanan sistem dari sisi *non repudiation* dalam validitas digital secara berkelanjutan.

Autentikasi penandatangan dan dokumen adalah alat untuk menghindari pemalsuan dan merupakan suatu penerapan konsep "*non-repudiation*" dalam bidang keamanan informasi. *Non-repudiation* adalah jaminan dari keaslian ataupun penyampaian dokumen asal untuk menghindari penyangkalan dari penandatangan dokumen (bahwa dia tidak menandatangani dokumen tersebut) serta penyangkalan dari pengirim dokumen (bahwa dia tidak mengirimkan dokumen tersebut) (Daffa et al., 2023).

## SIMPULAN

Analisis implementasi Rekam Medis Elektronik (RME) di RSUD Kabupaten Klungkung menunjukkan hasil yang beragam dalam aspek keamanan informasi. Dalam hal privasi, ancaman utama muncul dari kelalaian pengguna dalam menjaga kerahasiaan user dan password. Namun, untuk aspek integritas, sistem RME telah dilengkapi dengan notifikasi atau konfirmasi otomatis sebelum data disimpan, memastikan keakuratan dan tinjauan ulang informasi. Mekanisme autentikasi juga sudah memadai dengan penerapan username, password, dan tanda tangan elektronik pada setiap dokumen. Selain itu, ketersediaan data RME diakui penting untuk mutu layanan dan keselamatan pasien, didukung oleh kebutuhan pengembangan sistem dan peningkatan kapasitas. RSUD Kabupaten Klungkung juga telah menerapkan kontrol akses yang baik melalui tinjauan sistem dan penetapan peran serta tanggung jawab pengguna sesuai SK Direktur, serta memenuhi aspek non-repudiasi dengan penggunaan tanda tangan elektronik (TTE) dalam pengisian rekam medis.

## UCAPAN TERIMAKASIH

Ucapan Terima Kasih peneliti sampaikan pada semua pihak yang telah memberikan kontribusi dalam penyelesaian penelitian ini.

## DAFTAR PUSTAKA

Akraman, R., Candiwan, C., & Priyadi, Y. (2018). Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia. *Jurnal Sistem Informasi Bisnis*, *8*(2), 1. https://doi.org/10.21456/vol8iss2pp1-8

Andhani, A. Z. (2023). *Panduan Umum Dasar-dasar Rekam Medis*.

Ardianto, E. T., & Nurjanah, L. (2024). Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik Di Rumah Sakit X. *Jurnal Rekam Medik Dan Manajemen Informasi Kesehatan*, *3*(2), 18–30.

Aulia, A.-Z. R., & Sari, I. (2023). Analisis Rekam Medis Elektronik Dalam Menunjang Efektivitas Kerja di Unit Rekam Medis di Rumah Sakit Hermina Pasteur. *INFOKES*, *7*. https://journal.piksi.ac.id/index.php/INFOKES/article/view/1028/618

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology; In qualittaive research in psychology. *Uwe Bristol*, *3*(2), 77–101.

Budiman, A., Isa, M., & Soekiswati, S. (2025). Analisis Risiko Dan Tindakan Pencegahan Kebocoran Data Rekam Medis Elektronik Pasien Di RS P Surakarta. *Ranah Research*, *7*(3), 2118–2127.

Bustami, A., & Bahri, S. (2020). Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi : Systematic Review. *Unistek*, *7*(2), 59–70. https://doi.org/10.33592/unistek.v7i2.645

Gemawaty, C. A., & Yuliani, Y. (2024). *Manajemen Identitas dan Akses Dalam Keamanan Sistem Informasi (Pendekatan Literature Review)*. *4*(September), 396–403.

Koesmarijanto, Hidayati, N., Cahyani, D. D., & Anto, N. B. (2023). Smart Locker Menggunakan Fingerprint dan Face Recognition sebagai Sistem Keamanan Loker Penyimpanan. *Journal Of Applied Smart Electrical Network And Systems (JASENS)*, *4*(2), 68–76.

Listyorini, P. I. I. S. (2021). Sistem Keamanan SIMRS di Rumah Sakit. *Prosiding Seminar Informasi Kesehatan Nasional (SIKesNas)*, 234–240.

Madhrozji, T., & Effiyaldi. (2019). Informasi Administrasi Arsip Berbasis Web Pada Kantor Biro Pbmd Setda Provinsi. *Jurnal Manajemen Sistem Informasi*, *4*(3), 244–254. https://ejournal.unama.ac.id/index.php/jurnalmsi/article/download/1205/1014

Meilia, P. D. I., Christianto, G. M., & Librianty, N. (2019). Buah Simalakama Rekam Medis Elektronik: Manfaat Versus Dilema Etik. *Jurnal Etika Kedokteran Indonesia*, *3*(2), 61. https://doi.org/10.26880/jeki.v3i2.37

Nasution, A. F. (2023). *Metode Penelitian Kualitatif* (G. M. Albina, Zulfia, & Nita (eds.); pertama). CV. Harfa Creative.

Purwawijaya, E., Syahputra, D., Singarimbun, R. N., & Rambe, A. (2025). *Pelatihan Kesadaran Keamanan Informasi bagi Karyawan PT . Wijaya Kesuma Segara untuk Mencegah Ancaman Siber*. *2*(1), 50–55.

Rahman, F. (2021). *Analisa Dan Implementasi Single Sign on Dan Role-Based Access Control Pada Sistem Informasi Akademik (Studi Kasus: Uin Suska ...* [Universitas Islam Negeri Sultan Syarif Kasim Riau]. http://repository.uin-suska.ac.id/45107/%0Ahttp://repository.uin-suska.ac.id/45107/1/Laporan TA_Fathur Rahman.pdf

Rahmawati, F., Nazhifah Suryana, N., Gegerkalong Hilir, J., Parongpong, K., Bandung Barat, K., & Barat, J. (2024). Pentingnya Standar Operasional Prosedur (SOP) Dalam Meningkatkan Efisiensi Dan Konsistensi Operasional Pada Perusahaan Manufaktur D4 Administrasi Bisnis/Administrasi Niaga Politeknik Negeri Bandung. *Jurnal Manajemen Bisnis Digital Terkini (JUMBIDTER)*, *1*(3), 2–15. https://doi.org/10.61132/jumbidter.v1i2.112

Rizkinaswara, L. (2022). *Kominfo Merespons Dugaan Kebocoran Data Milik Kemenkes*.

Sahir, S. H. (2021). *Metodelogi Penelitian* (T. Koryati (ed.); Pertama). KBM Indonesia.

Santi Lestari, S., & Azizah, N. (2025). TINJAUAN PENERAPAN SISTEM INFORMASI REKAM MEDIS ELEKTRONIK TERHADAP KEAMANAN DATA PASIEN DI RUMAH SAKIT KARTINI RANGKASBITUNG. *EDU RMIK Jurnal Edukasi Rekam Medis Informasi Kesehatan*, *4*(1), 91–99.

Sari, I. C., Alvionita, C. V., & Gunawan. (2021). Literature Review Analisis Permasalahan Privasi Pada Rekam Medis Elektronik. *Jurnal Rekam Medis Dan Informasi Kesehatan Indonesia (Jurmiki)*, *1*(1), 47–56.

Simanjuntak, A., Sholikh, A. F., Tampubolon, E., & Br Sitepu, M. S. (2022). Hubungan Ekspektasi Usaha Dan Ekspektasi Kinerja Dengan Pemanfaatan Rekam Medik Elektronik Di Instalasi Rawat Jalan Rumah Sakit Umum Cut Meutia Kabupaten Aceh Utara Tahun 2022. *Jurnal Penelitian Kesmasy*, *5*(1), 49–57. https://doi.org/10.36656/jpksy.v5i1.1098

Sofia, S. (2022). *Analisis Aspek Keamanan Informasi Data Pribadi Pasien Pada Penerapan Rekam Medik Elektronik Di Fasilitas Kesehatan : Literature Review*.

Soraya, Nindya, E., & Mawan, M. S. A. (2025). Evaluasi Keamanan Dan Privasi Sistem Rekam Medis Elektronik : Studi Kasus Di Rumah Sakit Wava Husada Email : Ipesoraya@Gmail.Com Abstrak Pendahuluan Rumah Sakit Adalah Institusi Pelayanan Kesehatan Pelayanan Yang Menyelenggarakan Perorangan Standar Iso /. *Jrmik Stia Malang*.

Syahputra, R. A., Maliza, N. O., Kasmawati, & Putri, C. W. A. (2024). Strategi Peningkatan Kesadaran Data dan Informasi Masyarakat di Era Digital. *Jurnal Pengabdian Kepada Masyarakat Nusantara (JPkMN)*, *5*(3), 3164–3171.

Tiara, S., & Kinanti, M. C. (2023). *Determinan Kepercayaan Masyarakat terhadap Dorongan Penggunaan Telemedicine : Systematic Literature Review*. *December*.