

EVALUASI KEAMANAN DAN PRIVASI DATA PASIEN DALAM PENERAPAN REKAM MEDIS ELEKTRONIK

1. Eltigeka Devi Apriliani, Program Studi DIII Perekam dan Informasi Kesehatan, STIKES Bhakti Husada Mulia Madiun
2. Arvian Hadi Pratama, Program Studi DIII Perekam dan Informasi Kesehatan, STIKES Bhakti Husada Mulia Madiun
3. Eva Rusdianah, Program Studi DIII Perekam dan Informasi Kesehatan, STIKES Bhakti Husada Mulia Madiun
4. Umar Said, Program Studi DIII Perekam dan Informasi Kesehatan, STIKES Bhakti Husada Mulia Madiun

Korespondensi : eltigeka13@gmail.com

ABSTRAK

Perkembangan teknologi informasi yang pesat telah mendorong transformasi di berbagai sektor, termasuk di bidang kesehatan. Salah satu wujud nyata dari transformasi tersebut adalah peralihan sistem pencatatan medis dari metode manual berbasis kertas menuju rekam medis elektronik. Sistem ini memungkinkan pengelolaan data pasien secara terkomputerisasi, mulai dari pendaftaran, anamnesis, diagnosis, hingga tindakan pengobatan. Seiring berjalannya waktu, rekam medis elektronik tidak hanya berfungsi sebagai alat pencatatan, tetapi juga berkembang menjadi sistem informasi terintegrasi yang mendukung pengambilan keputusan klinis, peningkatan efisiensi pelayanan, dan kolaborasi antar tenaga kesehatan. Evaluasi keamanan dan privasi data pasien dalam rekam medis elektronik diperlukan untuk menjamin keamanan, kerahasiaan, keutuhan, ketersediaan data. Tujuan penelitian ini mengevaluasi keamanan dan privasi data pasien dalam rekam medis elektronik menggunakan aspek keamanan confidentiality, integrity, availability di RSUD X. Metode penelitian kualitatif, pengumpulan data dengan wawancara, observasi, dokumentasi. Informan dalam penelitian ini sebanyak 7 informan. Hasil penelitian aspek confidentiality tentang sistem perlindungan kerahasiaan data pasien yang diterapkan sudah baik, memiliki username, password, logout otomatis. Aspek integrity penetapan wewenang jelas dalam edit dan hapus data, terdapat pembatasan akses sesuai peran wewenang. Penggunaan fitur verifikasi data membantu menjaga keakuratan dan keutuhan informasi pasien. Aspek Availability penyediaan ketersediaan dan pencarian data rekam medis mudah diakses. Tersedia jaringan, penyimpanan data server internal dan ketentuan jadwal backup data yang terstruktur. Peningkatan pada aspek confidentiality terkait sistem keamanan dan perlindungan terhadap potensi kebocoran data dengan memperkuat pemantauan aktivitas pengguna serta melakukan pelatihan rutin bagi petugas yang menggunakan rekam medis elektronik.

Kata Kunci : Evaluasi, Keamanan, Confidentiality, Integrity, Availability

PENDAHULUAN

Rekam medis elektronik merupakan sebuah sistem pencatatan digital yang digunakan oleh fasilitas pelayanan kesehatan untuk mendokumentasikan secara komprehensif seluruh informasi terkait pasien, mulai dari data identitas diri, riwayat pemeriksaan klinis, prosedur pengobatan, hingga berbagai tindakan medis dan pelayanan lain yang diterima oleh pasien selama menjalani perawatan. Keberadaan sistem ini tidak hanya bertujuan untuk menggantikan catatan kertas konvensional, melainkan juga untuk meningkatkan mutu pelayanan melalui akses informasi yang cepat, akurat, dan terintegrasi (Permenkes, 2022). Dalam penerapannya, rekam medis elektronik harus dilandasi oleh tiga pilar utama keamanan informasi, yaitu kerahasiaan, integritas, dan ketersediaan data, yang secara bersama-sama berfungsi untuk menjamin bahwa data pasien terlindungi dari akses yang tidak sah, tetap utuh dan tidak mengalami perubahan yang tidak bertanggung jawab, serta selalu dapat diakses oleh pihak yang berwenang ketika dibutuhkan. Perlindungan data dalam konteks ini bukan semata masalah teknis, tetapi juga merupakan wujud penghormatan terhadap hak privasi pasien sebagai individu yang mempercayakan informasi kesehatannya kepada tenaga kesehatan. Dengan demikian, keamanan dan privasi data pasien dalam rekam medis elektronik menjadi fondasi etis dan operasional yang tidak dapat ditawar, karena setiap celah keamanan berpotensi mengancam tidak hanya kerahasiaan informasi, tetapi juga keselamatan pasien dan kepercayaan publik terhadap sistem pelayanan kesehatan secara keseluruhan (Tiorentap & Hosizah, 2020).

Keamanan data dalam sistem rekam medis elektronik pada hakikatnya merupakan upaya sistematis untuk melindungi setiap informasi sensitif dan data penting pasien dari berbagai ancaman, baik yang bersifat fisik maupun digital, seperti kerusakan, pencurian, kebocoran, maupun pemanfaatan oleh pihak yang tidak memiliki kewenangan. Penerapan sistem keamanan yang memadai tidak hanya berfungsi sebagai benteng teknis, tetapi juga sebagai jaminan bahwa data pasien tetap utuh, akurat, dan hanya dapat diakses oleh individu yang berhak sesuai dengan peran dan tanggung jawabnya dalam pelayanan kesehatan (Ujung *et. al.*, 2023). Dengan demikian, perlindungan data ini menjadi instrumen strategis untuk meminimalisasi tindak kejahatan terhadap data pribadi pasien, mengurangi potensi penyalahgunaan rekam medis di luar kepentingan pelayanan yang sah, serta mencegah perubahan informasi yang tidak sah karena setiap perubahan data hanya boleh dilakukan oleh pemilik informasi atau pihak yang diberi wewenang secara jelas. Lebih dari sekadar kepatuhan terhadap regulasi, keamanan data juga mencerminkan nilai humanisme dan penghormatan terhadap hak privasi pasien, karena setiap individu berhak atas kerahasiaan informasi kesehatannya dan kepercayaan yang diberikan kepada fasilitas pelayanan kesehatan harus dijaga dengan integritas tinggi. Dalam praktiknya, pemantauan dan evaluasi terhadap sistem rekam medis elektronik secara berkala menjadi langkah yang sangat penting untuk mendeteksi kerentanan sedini mungkin, sehingga risiko bahaya yang mengancam keamanan dan privasi data dapat diantisipasi dan diminimalisasi secara berkelanjutan (Pradita *et. al.*, 2022).

Pemantauan keamanan data pasien dalam sistem rekam medis elektronik merupakan kegiatan yang tidak dapat diabaikan karena berfungsi sebagai mekanisme pengendalian untuk memastikan bahwa seluruh informasi kesehatan tetap terjaga kerahasiaannya, keutuhannya, dan ketersediaannya sesuai dengan prinsip dasar perlindungan data. Kegiatan pemantauan ini

dilakukan secara berkesinambungan guna mendeteksi setiap potensi ancaman atau kelemahan sistem yang dapat membahayakan data pasien, sehingga tindakan perbaikan dapat segera dilakukan sebelum menimbulkan dampak yang lebih luas terhadap pelayanan kesehatan (Ardianto et al., 2024). Dalam konteks yang lebih luas, evaluasi terhadap keamanan dan privasi data memiliki manfaat yang sangat strategis, karena melalui evaluasi, fasilitas pelayanan kesehatan dapat memperoleh gambaran yang jelas mengenai sejauh mana pelaksanaan sistem keamanan telah berjalan, mengidentifikasi berbagai kendala yang dihadapi, serta merumuskan keputusan yang tepat berdasarkan hasil analisis dan diskusi bersama para pemangku kepentingan. Proses evaluasi ini pada akhirnya menjadi landasan bagi perbaikan dan penyempurnaan sistem secara terus menerus, yang bertujuan untuk meningkatkan kualitas pelayanan secara keseluruhan. Di balik aspek teknis dan manajerial tersebut, terdapat nilai humanisme yang mendasar, yaitu bahwa setiap upaya pemantauan dan evaluasi yang dilakukan pada hakikatnya adalah wujud tanggung jawab moral institusi pelayanan kesehatan kepada pasien sebagai subjek yang memiliki hak atas perlindungan data pribadinya, sehingga kepercayaan yang diberikan pasien kepada rumah sakit dapat terus terjaga dan diperkuat melalui perbaikan sistem yang berkelanjutan (Putri et. al., 2023).

Berdasarkan hasil wawancara yang telah dilaksanakan di RSUD X, diperoleh fakta bahwa institusi tersebut belum pernah melakukan evaluasi secara formal dan menyeluruh terkait dengan keamanan serta privasi data pasien dalam sistem rekam medis elektronik yang digunakannya, meskipun sistem tersebut telah diimplementasikan dan berjalan di unit pelayanan rawat jalan, sementara untuk pelayanan rawat inap penerapannya belum sepenuhnya menjangkau seluruh bagian. Dalam pengoperasiannya, setiap petugas diberikan akun akses berupa nama pengguna dan kata sandi yang berlaku pada masing masing unit pelayanan, dan sistem dilengkapi dengan mekanisme keluar otomatis apabila tidak digunakan dalam jangka waktu tertentu, yang bertujuan untuk mencegah akses tidak sah. Selain itu, terdapat pengaturan hak akses yang membedakan kewenangan setiap petugas, sehingga tindakan mengedit atau menghapus data hanya dapat dilakukan oleh pihak yang memiliki wewenang sesuai dengan peran dan tanggung jawabnya masing masing. Sistem rekam medis elektronik di rumah sakit tersebut dibangun dan dikelola oleh pihak ketiga atau vendor eksternal, yang berarti pengawasan dan pemeliharaan keamanan sistem sangat bergantung pada kerjasama dengan penyedia layanan tersebut. Dari sisi ketersediaan data, sistem dinilai mampu menyediakan informasi pasien dengan cepat dan terintegrasi antar poliklinik, sehingga mendukung kelancaran alur pelayanan. Namun demikian, fakta penting yang ditemukan adalah sistem pernah mengalami serangan peretasan yang mengakibatkan server mengalami gangguan hingga tidak berfungsi, yang pada akhirnya menghambat seluruh proses pelayanan kesehatan di rumah sakit. Kejadian ini menjadi sinyal kritis bahwa tanpa adanya evaluasi yang berkelanjutan terhadap aspek keamanan dan privasi data, risiko serupa dapat terulang kembali dan berpotensi mengancam tidak hanya kelangsungan operasional rumah sakit, tetapi juga keselamatan pasien serta kepercayaan masyarakat terhadap kualitas pelayanan yang diberikan.

Temuan berbagai permasalahan yang teridentifikasi dalam penerapan rekam medis elektronik menegaskan bahwa fasilitas pelayanan kesehatan memiliki tanggung jawab yang tidak dapat ditawar untuk secara terus menerus melakukan evaluasi terhadap aspek keamanan

dan privasi data pasien, karena evaluasi bukan sekadar kegiatan administratif, melainkan upaya strategis untuk memastikan bahwa setiap informasi kesehatan yang tersimpan dalam sistem digital benar benar terlindungi dari berbagai ancaman. Evaluasi yang berkelanjutan memungkinkan institusi untuk mendeteksi celah kelemahan sistem secara dini, memahami akar permasalahan yang timbul, dan merumuskan langkah langkah perbaikan yang tepat guna mencegah terulangnya insiden serupa di masa mendatang. Lebih dari itu, fasilitas pelayanan kesehatan dituntut untuk tidak hanya mengidentifikasi masalah, tetapi juga memberikan solusi konkret dan aplikatif yang mampu menyelesaikan permasalahan yang telah terjadi, terutama yang berkaitan dengan kerahasiaan, keutuhan, dan ketersediaan data pasien. Solusi yang ditawarkan harus mencakup aspek teknis seperti peningkatan infrastruktur keamanan sistem, aspek prosedural seperti penyusunan kebijakan internal yang lebih ketat, serta aspek sumber daya manusia melalui pelatihan dan peningkatan kesadaran petugas akan pentingnya perlindungan data. Di balik seluruh upaya teknis dan manajerial tersebut, terdapat nilai humanisme yang mendasar, yaitu bahwa setiap langkah evaluasi dan penyelesaian masalah yang dilakukan pada hakikatnya merupakan wujud penghormatan institusi terhadap hak privasi pasien dan komitmen untuk menjaga kepercayaan yang telah diberikan oleh masyarakat, karena pasien bukan sekadar objek pelayanan, melainkan subjek yang memiliki hak atas kerahasiaan informasi kesehatannya dan berhak mendapatkan perlindungan penuh dari setiap potensi penyalahgunaan data.

TUJUAN PENELITIAN

Tujuan penelitian ini adalah untuk mengevaluasi keamanan dan privasi data pasien dalam rekam medis elektronik menggunakan aspek confidentiality, integrity, availability di RSUD X.

METODE PENELITIAN

Penelitian ini dirancang dengan menggunakan pendekatan kualitatif yang bertujuan untuk mengevaluasi secara mendalam keamanan dan privasi data pasien dalam sistem rekam medis elektronik, dengan memfokuskan perhatian pada tiga aspek utama keamanan informasi, yaitu kerahasiaan, integritas, dan ketersediaan data. Pemilihan ketiga aspek tersebut didasarkan pada pertimbangan bahwa ketiganya merupakan pilar fundamental yang saling terkait dan secara bersama sama membentuk fondasi perlindungan data, sehingga melalui pengkajian yang terfokus pada masing masing aspek, penelitian ini diharapkan mampu memperoleh gambaran yang rinci, komprehensif, dan mendalam mengenai implementasi keamanan dalam pengelolaan data pasien di lingkungan rumah sakit. Untuk mendukung pencapaian tujuan tersebut, subjek penelitian ditentukan secara purposif dengan melibatkan para pemangku kepentingan yang secara langsung menggunakan dan mengelola sistem rekam medis elektronik, yang terdiri dari kepala rekam medis sebagai penanggung jawab administratif, dua orang petugas pendaftaran sebagai garda depan penerimaan data pasien, dua orang petugas teknologi informasi sebagai pengelola teknis sistem, serta dua orang petugas pemberi pelayanan sebagai pengguna akhir yang berinteraksi langsung dengan data klinis pasien. Keberagaman latar belakang dan peran subjek penelitian ini dipilih secara sengaja untuk menghasilkan perspektif yang holistik dan saling melengkapi, karena setiap petugas memiliki pengalaman, tantangan, dan pemahaman

yang berbeda mengenai keamanan data sesuai dengan posisi dan tanggung jawabnya masing-masing dalam rantai pelayanan. Pengumpulan data dilakukan melalui tiga teknik secara simultan, yaitu wawancara mendalam untuk menggali pandangan dan pengalaman subjek secara lisan, observasi langsung untuk mengamati praktik pengamanan data di lapangan, serta dokumentasi untuk menelusuri berbagai bukti tertulis dan catatan yang relevan dengan penerapan sistem. Dengan pendekatan yang menyeluruh ini, penelitian tidak hanya berorientasi pada aspek teknis keamanan sistem, tetapi juga memperhatikan dimensi manusiawi, karena di balik setiap data yang tersimpan terdapat individu pasien yang berhak atas perlindungan privasi, dan di balik setiap prosedur keamanan terdapat petugas yang memerlukan pemahaman serta kesadaran untuk menjalankan tanggung jawabnya dengan penuh integritas.

HASIL PENELITIAN

1. Penerapan Aspek Confidentiality

Petugas memiliki username dan password, setiap pengguna memiliki hak akses sesuai tugasnya, sehingga tidak semua data dapat diakses. Data pasien hanya bisa diakses oleh pihak yang berwenang sesuai dengan ketentuan. Loker pendaftaran hanya digunakan data dasar pasien, tanpa akses ke detail pelayanan medis. Setiap pengguna termasuk dokter, perawat, petugas rekam medis, diberikan username dan password unik, sehingga tidak dapat memodifikasi data tanpa izin. Ketentuan password terdiri dari kombinasi huruf besar, huruf kecil, angka, dengan panjang ideal antara 7 hingga 9 digit. Sistem memiliki batas waktu untuk login yaitu sekitar 5 hingga 10 menit, jika tidak ada aktivitas dalam waktu tersebut, sistem logout dan pengguna harus login kembali untuk mengakses. Secara umum sistem akan logout secara otomatis setelah periode waktu yang ditentukan. Akses sistem dibatasi untuk menjaga keamanan, pencatatan medis dilakukan dokter setelah pelayanan diberikan. Hak akses penuh diberikan kepada dokter dan pimpinan yang terlibat langsung dalam perawatan pasien. Terdapat proteksi tambahan pada server untuk memastikan bahwa hanya pengguna tertentu dari pihak IT yang dapat mengakses database. Akses data hanya diperbolehkan untuk keperluan medis atau hukum yang sah. Semua petugas RSUD mengakses sistem rekam medis sesuai kebutuhan pelayanan dan wajib melindungi data pasien terhadap potensi kebocoran data.

2. Penerapan Aspek Integrity

Pengaturan rekam medis elektronik di RSUD sangat ketat. Pihak yang berwenang, seperti dokter dan administrator memiliki akses untuk mengubah data. Petugas kesehatan seperti perawat dapat mengedit informasi terkait tindakan pasien, tetapi tidak dapat mengubah data di luar tanggungjawab. Penemuan kasus pada rekam medis elektronik ialah terjadi kesalahan dalam pencatatan keluhan pasien, maka petugas harus segera melakukan perbaikan dengan mengedit data yang telah disimpan sebelum pasien dinyatakan pulang. Hak akses yang berhak mengubah atau mengedit data rekam medis elektronik sesuai tugas yang berwenang. Data rekam medis tidak dapat diubah jika pasien tersebut dinyatakan pulang dan hanya admin dari Petugas IT yang memiliki akses untuk melakukan perubahan. Pengelolaan data rekam medis elektronik belum lengkap maka petugas akan mengembalikan kepada perawat atau dokter yang bertanggung jawab untuk melengkapi

informasi. Setiap data yang dimasukkan ke dalam sistem harus akurat, mengingat pentingnya dokumentasi rekam medis. Petugas pendaftaran bertanggung jawab untuk memastikan bahwa data yang dimasukkan tidak salah dan melakukan verifikasi dengan dokter jika ada kesalahan yang perlu diperbaiki. Sistem rekam medis elektronik dilengkapi dengan fitur verifikasi untuk memastikan kelengkapan data. Petugas setelah mengisi formulir, pengguna dapat melihat status pengisian yang menunjukkan data sudah terisi dan belum. Informasi penting seperti nomor NIK tidak lengkap, maka data tidak dapat disimpan. Petunjuk pengisian kelengkapan data ialah ikon centang atau huruf berwarna merah untuk menandai bagian yang belum lengkap dalam sistem.

3. Penerapan Aspek Availability

Data rekam medis elektron disimpan pada server internal untuk menjaga keamanan data pasien. Sistem rekam medis elektronik masih baru dan dikelola bersama pihak ketiga (vendor). Pihak IT bertanggung jawab untuk melakukan backup data secara otomatis setiap malam pada pukul 00.00. Backup ini penting untuk mencegah kehilangan data akibat kerusakan atau kebocoran. Pihak IT dapat memeriksa dan mengembalikan data dari cadangan yang telah disimpan, jika terjadi kehilangan data. Dokter poli memiliki tugas utama memasukkan dan menginput data pasien, sementara pemeliharaan dan keamanan data menjadi tanggungjawab Petugas IT. Ketersediaan jaringan pada rekam medis elektronik cek secara berkala. Permintaan data pasien dalam keadaan darurat hanya dapat diakses oleh petugas yang berwenang dan harus didokumentasikan dengan jelas. Prosedur yang harus diikuti melibatkan verifikasi identitas dan alasan permintaan, serta penyediaan data yang terbatas dan relevan. Dokter atau tenaga medis yang menangani pasien diberikan akses langsung ke data yang diperlukan, termasuk rekam medis sebelumnya, akses hanya diberikan untuk data minimal yang dibutuhkan untuk menyelamatkan nyawa pasien. Rekam medis elektronik dapat menyediakan data sesuai keperluan pasien dengan syarat sesuai prosedur yang ditetapkan.

PEMBAHASAN

1. Penerapan Aspek Confidentiality

Dalam penerapan aspek kerahasiaan data, setiap petugas di RSUD X diberikan nama pengguna dan kata sandi yang bersifat unik sebagai identitas digital untuk mengakses sistem rekam medis elektronik, di mana hak akses yang dimiliki oleh masing masing pengguna disesuaikan secara ketat dengan tugas dan tanggung jawabnya masing masing, sehingga tidak seluruh data pasien dapat diakses oleh semua petugas melainkan hanya oleh pihak pihak yang memiliki kewenangan sesuai dengan ketentuan yang berlaku. Sebagai contoh, petugas di loket pendaftaran hanya diperkenankan mengakses data dasar pasien seperti identitas diri, tanpa memiliki akses terhadap rincian pelayanan medis yang lebih mendalam, sementara tenaga medis seperti dokter dan perawat serta petugas rekam medis masing masing memiliki tingkat akses yang berbeda sesuai dengan kebutuhan pelayanan mereka. Untuk memperkuat keamanan akses, sistem menerapkan kebijakan kata sandi yang mengharuskan kombinasi huruf besar, huruf kecil, dan angka dengan panjang ideal antara tujuh hingga sembilan digit, sehingga mengurangi risiko peretasan akun pengguna.

Selain itu, sistem dilengkapi dengan mekanisme keluar otomatis yang aktif apabila tidak ada aktivitas dalam rentang waktu lima hingga sepuluh menit, yang mengharuskan pengguna untuk melakukan proses masuk kembali guna memastikan bahwa akses yang terbuka tidak dimanfaatkan oleh pihak yang tidak berwenang. Hak akses penuh terhadap sistem hanya diberikan kepada dokter dan pimpinan yang terlibat langsung dalam proses perawatan pasien, sedangkan untuk perlindungan pada tingkat server, diterapkan proteksi tambahan yang membatasi akses ke basis data hanya untuk petugas teknologi informasi tertentu. Seluruh akses terhadap data pasien hanya diperbolehkan untuk kepentingan medis atau keperluan hukum yang sah, dan setiap petugas di lingkungan rumah sakit memiliki kewajiban untuk melindungi informasi pasien dari potensi kebocoran data sebagai bentuk tanggung jawab profesional dan moral. Di balik seluruh kebijakan teknis tersebut, terdapat nilai humanisme yang mendasar, yaitu bahwa setiap lapisan perlindungan yang diterapkan pada hakikatnya adalah wujud penghormatan terhadap hak privasi pasien sebagai individu yang mempercayakan informasi kesehatannya kepada institusi pelayanan kesehatan, sehingga kerahasiaan data bukan sekadar kepatuhan terhadap aturan, melainkan cerminan integritas dan komitmen etis dalam menjaga kepercayaan yang telah diberikan masyarakat.

Konsep kerahasiaan data dalam sistem informasi kesehatan menekankan bahwa perlindungan terhadap informasi pasien harus dibangun melalui lapisan keamanan yang saling memperkuat, dimulai dari otentikasi pengguna, otorisasi akses, hingga pengendalian sesi dan perlindungan infrastruktur (Tiorentap & Hosizah, 2020). Prinsip dasar yang melandasi aspek kerahasiaan adalah bahwa setiap individu memiliki hak fundamental atas privasi informasi kesehatannya, dan hak tersebut hanya dapat dikecualikan apabila terdapat kepentingan medis atau hukum yang sah dan telah diatur secara jelas dalam kebijakan institusi. Dalam konteks rekam medis elektronik, penerapan kerahasiaan data tidak cukup hanya dengan memberikan nama pengguna dan kata sandi, karena sistem harus mampu membedakan tingkat akses setiap pengguna berdasarkan peran dan tanggung jawabnya sehingga informasi hanya tersedia bagi pihak yang benar benar membutuhkannya. Kebijakan kata sandi yang kompleks, mekanisme keluar otomatis, pembatasan akses berdasarkan peran, serta proteksi server merupakan elemen elemen teknis yang secara bersama sama membentuk sistem pertahanan berlapis untuk mencegah akses tidak sah dan kebocoran data (Ujung *et. al.*, 2023). Namun demikian, keamanan teknis saja tidak cukup tanpa didukung oleh kesadaran etis setiap petugas yang mengakses sistem, karena kerahasiaan data pada hakikatnya adalah tanggung jawab moral yang melekat pada profesi kesehatan. Dengan demikian, teori keamanan informasi menempatkan aspek kerahasiaan sebagai pilar yang tidak hanya bersifat teknokratis, tetapi juga humanistik, karena setiap kebijakan perlindungan data pada akhirnya bermuara pada penghormatan terhadap martabat dan hak privasi pasien (Ardianto *et al.*, 2024).

Berdasarkan hasil temuan di RSUD X, peneliti berasumsi bahwa sistem keamanan yang diterapkan pada aspek kerahasiaan data telah dirancang dengan mempertimbangkan prinsip hak akses minimal, di mana setiap petugas hanya diberikan akses sesuai dengan kebutuhan pelayanannya, dan hal ini tercermin dari perbedaan tingkat akses antara petugas pendaftaran yang hanya dapat mengakses data dasar, dengan tenaga medis dan

pimpinan yang memperoleh akses lebih luas. Asumsi peneliti selanjutnya adalah bahwa kebijakan kata sandi yang mengharuskan kombinasi huruf besar, huruf kecil, dan angka dengan panjang tujuh hingga sembilan digit, serta mekanisme keluar otomatis dalam waktu lima hingga sepuluh menit, menunjukkan adanya kesadaran institusi terhadap pentingnya pengendalian sesi untuk mencegah akses yang tidak bertanggung jawab, terutama dalam lingkungan pelayanan yang sibuk dan melibatkan banyak petugas. Namun demikian, peneliti juga mengasumsikan bahwa meskipun kebijakan teknis telah diterapkan, kepatuhan petugas dalam praktik sehari-hari tetap menjadi faktor kritis yang perlu dicermati, karena sistem keamanan terbaik sekalipun dapat menjadi lemah apabila petugas tidak disiplin dalam menjaga kerahasiaan kata sandi atau meninggalkan sesi login dalam keadaan terbuka. Perlindungan tambahan pada tingkat server yang membatasi akses basis data hanya untuk petugas teknologi informasi tertentu dinilai sebagai langkah strategis untuk mencegah intervensi teknis dari pihak yang tidak berwenang, namun efektivitas langkah ini sangat bergantung pada kompetensi dan integritas petugas teknologi informasi dalam menjalankan pengawasan terhadap database. Peneliti juga menganalisis bahwa pembatasan akses data hanya untuk kepentingan medis atau hukum yang sah merupakan bentuk implementasi dari prinsip proporsionalitas, di mana akses terhadap informasi sensitif tidak diberikan secara bebas melainkan harus didasarkan pada justifikasi yang jelas dan dapat dipertanggungjawabkan.

Analisis lebih lanjut dari temuan penelitian menunjukkan bahwa meskipun RSUD X telah menerapkan berbagai mekanisme perlindungan kerahasiaan data yang tergolong komprehensif, terdapat celah yang perlu mendapatkan perhatian serius, yaitu belum adanya sistem pemantauan aktivitas pengguna yang dapat merekam dan menganalisis setiap akses terhadap data pasien secara real time, sehingga jika terjadi pelanggaran, institusi tidak memiliki jejak audit yang cukup untuk melacak pihak yang bertanggung jawab. Peneliti menganalisis bahwa ketiadaan sistem pemantauan aktivitas ini menjadi titik lemah yang berpotensi mengurangi efektivitas seluruh lapisan keamanan yang telah dibangun, karena tanpa adanya pengawasan yang berkelanjutan, kepatuhan petugas terhadap kebijakan keamanan sulit untuk diukur dan dievaluasi secara objektif. Peneliti juga berasumsi bahwa kebutuhan akan pelatihan rutin bagi seluruh petugas pengguna sistem menjadi sangat mendesak, mengingat keamanan data tidak semata tergantung pada kecanggihan teknologi, tetapi juga pada tingkat kesadaran dan pemahaman setiap individu terhadap pentingnya melindungi informasi pasien dari potensi kebocoran. Dalam perspektif humanisme, peneliti menilai bahwa seluruh upaya teknis yang telah diterapkan oleh RSUD X sejatinya telah mencerminkan komitmen institusi untuk menghormati hak privasi pasien, namun komitmen tersebut perlu diperkuat dengan budaya organisasi yang menempatkan perlindungan data sebagai nilai etis yang dijunjung tinggi oleh seluruh komponen rumah sakit. Implikasi dari analisis ini menunjukkan bahwa RSUD X perlu mengembangkan sistem pemantauan aktivitas pengguna, menyusun program pelatihan berkelanjutan mengenai keamanan data, serta memperkuat kebijakan internal yang mengatur sanksi bagi pelanggaran kerahasiaan, sehingga aspek kerahasiaan data tidak hanya menjadi prosedur teknis yang tertulis di atas kertas, tetapi benar-benar terinternalisasi dalam praktik

pelayanan sehari-hari dan menjadi bagian dari budaya keselamatan pasien secara menyeluruh.

2. Penerapan Aspek Integrity

Dalam penerapan aspek integritas data, pengelolaan rekam medis elektronik di RSUD X dilakukan dengan tingkat ketelitian dan pengawasan yang sangat ketat, di mana wewenang untuk mengubah atau mengedit data hanya diberikan kepada pihak-pihak yang memiliki tanggung jawab langsung terhadap proses pelayanan kesehatan, seperti dokter dan administrator sistem, sedangkan tenaga kesehatan seperti perawat diberikan hak akses terbatas untuk mengedit informasi yang berkaitan dengan tindakan keperawatan yang menjadi tanggung jawabnya tanpa dapat mengubah data di luar cakupan tugas tersebut. Apabila terjadi kesalahan dalam pencatatan, misalnya keluhan pasien yang tidak sesuai dengan hasil anamnesis, maka petugas yang bersangkutan wajib segera melakukan perbaikan dengan mengedit data yang telah tersimpan selama pasien masih dalam masa perawatan dan belum dinyatakan pulang, karena setelah pasien dinyatakan pulang, data rekam medis tidak dapat diubah lagi dan hanya administrator dari petugas teknologi informasi yang memiliki kewenangan untuk melakukan perubahan dengan prosedur khusus. Dalam hal ditemukan data rekam medis yang belum lengkap, petugas akan mengembalikan dokumen tersebut kepada perawat atau dokter yang bertanggung jawab untuk melengkapi informasi yang diperlukan, karena setiap data yang dimasukkan ke dalam sistem harus memenuhi standar akurasi dan kelengkapan mengingat dokumentasi rekam medis memiliki kedudukan yang sangat penting sebagai dasar pengambilan keputusan klinis dan perlindungan hukum bagi kedua belah pihak. Petugas pendaftaran juga memiliki tanggung jawab untuk memastikan bahwa data yang dimasukkan tidak mengandung kesalahan dan melakukan verifikasi dengan dokter apabila ditemukan kekeliruan yang perlu diperbaiki, sehingga tercipta rantai pengawasan yang saling melengkapi antar petugas. Untuk mendukung upaya tersebut, sistem rekam medis elektronik dilengkapi dengan fitur verifikasi yang memungkinkan pengguna untuk melihat status pengisian data, baik yang sudah terisi maupun yang masih kosong, melalui indikator visual seperti ikon centang atau huruf berwarna merah yang secara jelas menandai bagian-bagian yang belum lengkap, bahkan data dengan informasi penting seperti nomor induk kependudukan tidak dapat disimpan ke dalam sistem apabila masih kosong. Di balik seluruh prosedur teknis dan administrative tersebut, terdapat nilai humanisme yang mendalam, karena setiap upaya untuk menjaga keutuhan dan keakuratan data pada hakikatnya adalah bentuk perlindungan terhadap hak pasien atas informasi kesehatannya yang benar dan dapat dipertanggungjawabkan, serta mencerminkan komitmen institusi untuk memberikan pelayanan yang bermutu dengan landasan data yang valid, sehingga setiap keputusan medis yang diambil berdasarkan rekam medis elektronik benar-benar demi kepentingan terbaik bagi keselamatan pasien.

Konsep integritas data dalam sistem informasi kesehatan menekankan bahwa setiap informasi yang tercatat dalam rekam medis elektronik harus akurat, utuh, dan tidak mengalami perubahan yang tidak sah atau tidak bertanggung jawab, karena keakuratan data merupakan fondasi utama bagi pengambilan keputusan klinis yang tepat dan

perlindungan hukum bagi tenaga kesehatan maupun pasien (Pradita *et. al.*, 2022). Prinsip dasar yang melandasi aspek integritas adalah bahwa data yang dimasukkan ke dalam sistem harus mencerminkan keadaan pasien yang sebenarnya pada saat pelayanan diberikan, dan setiap perubahan terhadap data tersebut harus dilakukan melalui mekanisme yang terkendali, transparan, dan dapat dipertanggungjawabkan. Dalam konteks rekam medis elektronik, penerapan integritas data tidak hanya bergantung pada pengaturan hak akses yang membatasi siapa yang dapat mengubah informasi, tetapi juga pada prosedur yang mengatur kapan dan dalam kondisi apa perubahan dapat dilakukan, serta siapa yang berwenang melakukannya (Agustina *et. al.* 2023). Dokumen rekam medis memiliki kedudukan yang sangat penting sebagai alat bukti hukum dan dasar evaluasi pelayanan, sehingga setiap kesalahan atau ketidaklengkapan data dapat berakibat fatal terhadap keselamatan pasien dan kredibilitas institusi. Oleh karena itu, sistem rekam medis elektronik harus dilengkapi dengan mekanisme verifikasi dan validasi data yang memastikan bahwa informasi yang disimpan telah memenuhi standar kelengkapan dan keakuratan sebelum data tersebut diterima sebagai dokumen resmi (Vansuri *et al.*, 2023). Dengan demikian, teori integritas data menempatkan perlindungan terhadap keutuhan informasi sebagai tanggung jawab bersama yang melibatkan seluruh petugas dalam rantai pelayanan, karena setiap data yang salah atau tidak lengkap dapat mengancam kualitas pelayanan dan merugikan pasien sebagai subjek yang berhak mendapatkan informasi kesehatan yang benar (Suhariyono *et. al.*, 2025).

Berdasarkan hasil temuan di RSUD X, peneliti berasumsi bahwa institusi telah memahami urgensi integritas data dengan menerapkan pembatasan wewenang yang jelas di mana dokter dan administrator sistem memiliki akses penuh untuk mengubah data, sementara perawat hanya diperkenankan mengedit informasi yang berkaitan dengan tindakan keperawatan sesuai dengan tanggung jawabnya, sehingga setiap perubahan data dapat dilacak dan dipertanggungjawabkan kepada pihak yang berwenang. Asumsi peneliti selanjutnya adalah bahwa kebijakan yang melarang perubahan data setelah pasien dinyatakan pulang, kecuali oleh administrator teknologi informasi dengan prosedur khusus, merupakan bentuk perlindungan terhadap keabsahan dokumen rekam medis sebagai bukti hukum yang sah, karena setelah pasien pulang, rekam medis dianggap sebagai dokumen final yang tidak dapat diubah secara sembarangan. Peneliti juga mengasumsikan bahwa mekanisme pengembalian data yang belum lengkap kepada perawat atau dokter yang bertanggung jawab untuk dilengkapi menunjukkan adanya rantai pengawasan yang saling melengkapi antar petugas, yang bertujuan untuk memastikan bahwa setiap informasi yang masuk ke dalam sistem telah memenuhi standar akurasi dan kelengkapan sebelum digunakan sebagai dasar pelayanan selanjutnya. Namun demikian, peneliti menganalisis bahwa efektivitas mekanisme ini sangat bergantung pada kesadaran dan kedisiplinan setiap petugas dalam menjalankan tanggung jawabnya masing masing, karena tanpa pengawasan yang ketat, potensi kelalaian dalam pengisian data tetap dapat terjadi dan berisiko mengganggu keutuhan informasi pasien. Peneliti juga menilai bahwa keterlibatan petugas pendaftaran dalam proses verifikasi data dengan dokter apabila ditemukan kekeliruan merupakan langkah positif yang menciptakan kolaborasi antar unit dalam menjaga

integritas data, namun langkah ini perlu didukung oleh komunikasi yang efektif dan prosedur yang baku agar proses verifikasi tidak menjadi hambatan dalam kelancaran pelayanan.

Analisis lebih lanjut dari temuan penelitian menunjukkan bahwa fitur verifikasi yang dilengkapi dengan indikator visual seperti ikon centang dan huruf berwarna merah untuk menandai bagian yang belum lengkap, serta penolakan sistem terhadap penyimpanan data apabila informasi penting seperti nomor induk kependudukan kosong, merupakan inovasi teknis yang sangat membantu petugas dalam memastikan kelengkapan data sebelum dokumen disimpan secara permanen. Peneliti menganalisis bahwa meskipun fitur tersebut telah diterapkan dengan baik, tantangan utama yang dihadapi adalah konsistensi petugas dalam memanfaatkan fitur verifikasi secara optimal, karena dalam situasi pelayanan yang padat, petugas cenderung terburu-buru dan berpotensi mengabaikan indikator kelengkapan yang ditampilkan oleh sistem. Peneliti juga berasumsi bahwa diperlukan mekanisme umpan balik yang lebih proaktif dari sistem, misalnya peringatan otomatis yang lebih tegas atau blokir penyimpanan data secara total apabila masih terdapat bagian yang belum lengkap, sehingga petugas tidak memiliki pilihan selain melengkapi data sebelum melanjutkan proses pelayanan. Dalam perspektif humanisme, peneliti menilai bahwa seluruh upaya menjaga integritas data yang dilakukan oleh RSUD X pada hakikatnya adalah bentuk tanggung jawab moral institusi terhadap pasien, karena setiap data yang akurat dan lengkap akan menghasilkan keputusan medis yang tepat, yang pada akhirnya berkontribusi pada keselamatan dan kesembuhan pasien. Implikasi dari analisis ini menunjukkan bahwa RSUD X perlu terus memperkuat sosialisasi dan pelatihan mengenai pentingnya pengisian data yang akurat dan lengkap, menyusun mekanisme evaluasi berkala terhadap kepatuhan petugas dalam menggunakan fitur verifikasi, serta mengembangkan sistem peringatan dini yang lebih efektif untuk mencegah terjadinya kesalahan atau ketidaklengkapan data yang dapat membahayakan pasien dan merugikan institusi di kemudian hari.

3. Penerapan Aspek Availability

Dalam penerapan aspek ketersediaan data, sistem rekam medis elektronik di RSUD X dirancang dengan memanfaatkan server internal sebagai tempat penyimpanan utama yang bertujuan untuk menjaga keamanan dan pengendalian data pasien secara lebih optimal, meskipun sistem tersebut masih tergolong baru dan pengelolaannya dilakukan bersama pihak ketiga atau vendor sebagai mitra teknis. Untuk mencegah kehilangan data akibat kerusakan sistem, kebocoran, atau insiden tidak terduga lainnya, petugas teknologi informasi memiliki tanggung jawab untuk melakukan pencadangan data secara otomatis setiap malam pada pukul 00.00, sehingga apabila terjadi kehilangan data, pihak teknologi informasi dapat memeriksa dan memulihkan data dari cadangan yang telah disimpan untuk memastikan kelangsungan pelayanan tidak terganggu. Pembagian peran dalam pengelolaan sistem juga dilakukan secara jelas, di mana dokter di poliklinik memiliki tugas utama untuk memasukkan dan menginput data pasien sebagai bagian dari proses pelayanan klinis, sementara pemeliharaan teknis dan keamanan data secara keseluruhan menjadi tanggung jawab petugas teknologi informasi yang memastikan sistem selalu dalam kondisi siap pakai. Ketersediaan jaringan juga dipantau dan diperiksa secara berkala oleh tim teknologi

informasi untuk mengantisipasi potensi gangguan yang dapat menghambat akses petugas terhadap data pasien, terutama dalam situasi darurat di mana permintaan data hanya dapat diakses oleh petugas yang berwenang dengan prosedur yang ketat, yaitu melalui verifikasi identitas peminta dan alasan permintaan yang jelas, serta penyediaan data yang dibatasi hanya pada informasi yang paling relevan dan minimal diperlukan untuk menyelamatkan nyawa pasien. Dokter atau tenaga medis yang menangani pasien dalam kondisi kritis diberikan akses langsung ke data yang diperlukan, termasuk rekam medis sebelumnya, namun akses tersebut tetap dibatasi hanya pada data minimal yang dibutuhkan untuk mendukung tindakan penyelamatan. Secara keseluruhan, sistem rekam medis elektronik mampu menyediakan data sesuai dengan keperluan pasien selama prosedur yang ditetapkan dipatuhi oleh seluruh petugas. Di balik seluruh mekanisme teknis yang telah diuraikan, terdapat nilai humanisme yang sangat mendasar, karena setiap upaya untuk memastikan ketersediaan data pada hakikatnya adalah wujud kesiapan institusi dalam memberikan pelayanan yang cepat dan tepat kepada pasien, terutama dalam situasi kritis di mana setiap detik sangat berharga, sehingga kehadiran data yang akurat dan mudah diakses menjadi bagian dari upaya menyelamatkan nyawa dan menjaga martabat pasien sebagai manusia yang membutuhkan pertolongan.

Konsep ketersediaan data dalam sistem informasi kesehatan menekankan bahwa data pasien harus selalu dapat diakses oleh pihak yang berwenang ketika dibutuhkan, terutama dalam situasi darurat di mana setiap detik sangat berharga bagi keselamatan pasien. Prinsip dasar yang melandasi aspek ketersediaan adalah bahwa sistem rekam medis elektronik tidak boleh mengalami gangguan yang menghambat akses petugas terhadap informasi kesehatan, karena keterlambatan dalam memperoleh data dapat berakibat fatal terhadap proses pengambilan keputusan klinis dan tindakan medis yang harus segera diberikan (Putri *et. al.*, 2023). Dalam konteks rekam medis elektronik, penerapan ketersediaan data tidak hanya bergantung pada infrastruktur teknologi seperti server, jaringan, dan perangkat keras, tetapi juga pada mekanisme pencadangan data, prosedur pemulihan bencana, serta pembagian peran yang jelas antara pengguna klinis dan pengelola teknis system (Suhariyono *et. al.*, 2025). Server internal sebagai tempat penyimpanan utama memberikan kendali penuh kepada institusi terhadap data pasien, namun pengelolaan yang melibatkan pihak ketiga atau vendor menuntut adanya kesepakatan yang jelas mengenai tanggung jawab teknis dan jaminan ketersediaan layanan. Pencadangan data secara terjadwal merupakan langkah preventif yang sangat penting untuk mencegah kehilangan data permanen akibat kerusakan sistem atau insiden siber, sedangkan pemantauan jaringan secara berkala berfungsi untuk mendeteksi potensi gangguan sebelum berdampak luas terhadap pelayanan (Budiman *et al.*, 2025). Dengan demikian, teori ketersediaan data menempatkan kesiapan teknis dan prosedural sebagai bagian yang tidak terpisahkan dari upaya institusi dalam memberikan pelayanan kesehatan yang berkualitas, karena ketersediaan data bukan sekadar masalah teknis, melainkan masalah keselamatan pasien yang menyangkut nyawa manusia (Ardianto *et al.*, 2024).

Berdasarkan hasil temuan di RSUD X, peneliti berasumsi bahwa pemilihan server internal sebagai tempat penyimpanan utama data rekam medis elektronik merupakan

keputusan strategis yang bertujuan untuk memberikan kendali penuh kepada institusi atas keamanan dan pengelolaan data pasien, meskipun keterlibatan pihak ketiga atau vendor dalam pengelolaan sistem menunjukkan bahwa rumah sakit masih memerlukan dukungan teknis eksternal yang perlu dikelola dengan baik melalui perjanjian kerjasama yang mengatur standar pelayanan dan tanggung jawab masing masing pihak. Asumsi peneliti selanjutnya adalah bahwa pencadangan data secara otomatis setiap malam pada pukul 00.00 menunjukkan adanya kesadaran institusi terhadap pentingnya perlindungan data dari risiko kehilangan, dan mekanisme ini dinilai cukup baik karena dilakukan secara rutin dan terstruktur, sehingga apabila terjadi insiden yang mengakibatkan hilangnya data, petugas teknologi informasi dapat segera memulihkan data dari cadangan yang telah disimpan untuk memastikan kelangsungan pelayanan tidak terganggu. Peneliti juga mengasumsikan bahwa pembagian peran yang jelas antara dokter yang bertugas menginput data pasien dan petugas teknologi informasi yang bertanggung jawab atas pemeliharaan serta keamanan sistem merupakan langkah yang tepat untuk menghindari tumpang tindih tanggung jawab dan memastikan bahwa setiap pihak fokus pada kompetensi utamanya masing masing. Namun demikian, peneliti menganalisis bahwa efektivitas mekanisme pencadangan dan pemulihan data sangat bergantung pada ketersediaan infrastruktur pendukung seperti ruang penyimpanan cadangan yang memadai dan prosedur pemulihan yang teruji secara berkala, karena tanpa pengujian rutin, cadangan data dapat saja tidak berfungsi ketika benar benar dibutuhkan. Peneliti juga menilai bahwa pemantauan jaringan secara berkala yang dilakukan oleh tim teknologi informasi merupakan upaya preventif yang penting untuk mengantisipasi gangguan akses, namun perlu dipastikan bahwa pemantauan tersebut mencakup seluruh komponen sistem termasuk koneksi antar unit pelayanan, sehingga tidak ada bagian yang terlewat dan berpotensi mengganggu ketersediaan data di titik titik kritis pelayanan.

Analisis lebih lanjut dari temuan penelitian menunjukkan bahwa prosedur akses data dalam situasi darurat yang melibatkan verifikasi identitas dan alasan permintaan, serta pembatasan data hanya pada informasi yang paling relevan dan minimal diperlukan untuk menyelamatkan nyawa pasien, merupakan bentuk keseimbangan antara prinsip ketersediaan dan prinsip kerahasiaan, di mana dalam kondisi kritis, akses terhadap data tetap diberikan namun dengan tetap memperhatikan batasan batasan yang melindungi privasi pasien. Peneliti menganalisis bahwa kebijakan ini mencerminkan pemahaman institusi bahwa dalam situasi darurat, kecepatan akses data tidak boleh mengorbankan prinsip perlindungan data, sehingga prosedur yang diterapkan harus mampu menjawab kedua kebutuhan tersebut secara simultan. Peneliti juga berasumsi bahwa akses langsung yang diberikan kepada dokter atau tenaga medis yang menangani pasien kritis terhadap rekam medis sebelumnya merupakan langkah yang sangat krusial untuk mendukung kontinuitas perawatan, karena informasi tentang riwayat penyakit, alergi, atau pengobatan sebelumnya sangat menentukan tindakan yang tepat dalam situasi gawat darurat. Namun demikian, peneliti mengidentifikasi bahwa temuan mengenai sistem yang pernah mengalami serangan peretasan yang mengakibatkan server down dan menghambat pelayanan merupakan sinyal kritis yang menunjukkan bahwa aspek ketersediaan data

masih memiliki celah yang signifikan, karena serangan siber tidak hanya mengancam kerahasiaan dan integritas data, tetapi juga secara langsung melumpuhkan ketersediaan data yang sangat vital bagi kelangsungan pelayanan kesehatan. Dalam perspektif humanisme, peneliti menilai bahwa seluruh upaya yang dilakukan RSUD X untuk memastikan ketersediaan data, mulai dari penyimpanan server internal, pencadangan rutin, pemantauan jaringan, hingga prosedur akses darurat, pada hakikatnya adalah wujud tanggung jawab institusi untuk memastikan bahwa setiap pasien mendapatkan pelayanan yang cepat dan tepat tanpa hambatan yang disebabkan oleh kegagalan teknis. Implikasi dari analisis ini menunjukkan bahwa RSUD X perlu segera memperkuat sistem keamanan siber untuk mencegah terulangnya serangan peretasan, mengembangkan rencana pemulihan bencana yang teruji, serta meningkatkan koordinasi dengan vendor dalam hal pemeliharaan dan peningkatan kapasitas sistem, sehingga ketersediaan data pasien dapat terjamin secara berkelanjutan dan pelayanan kesehatan tidak lagi terhambat oleh insiden teknis yang sebenarnya dapat diantisipasi.

KESIMPULAN

1. Aspek Confidentiality terkait pengguna sudah memiliki username dan password, logout secara otomatis jika meninggalkan aplikasi dalam waktu lama. Semua petugas dapat mengakses rekam medis elektronik sesuai kebutuhan pelayanan, wajib melindungi keamanan dan privasi data pasien.
2. Aspek Integrity terkait hak akses untuk edit dan hapus dapat dilakukan sesuai yang memiliki kewenangan. Terdapat fitur verifikasi untuk memastikan kelengkapan data rekam medis elektronik.
3. Aspek Availability terkait penyimpanan data rekam medis elektronik pada server internal. Petugas IT bertanggungjawab penuh melakukan backup data secara otomatis setiap malam untuk mencegah kehilangan atau kebocoran data pasien. Ketersediaan dan pencarian data rekam medis elektronik dalam keadaan darurat mudah diakses oleh petugas yang berwenang

SARAN

Peningkatan aspek confidentiality terkait sistem keamanan dan perlindungan terhadap potensi kebocoran data. Pemeliharaan sistem dan proses backup data dilaksanakan secara konsisten dan terjadwal untuk memastikan ketersediaan data setiap saat, termasuk dalam kondisi darurat. Mempertimbangkan penerapan sistem otentikasi ganda (two-factor authentication) untuk meningkatkan keamanan login. Petugas IT dapat memperkuat pemantauan aktivitas pengguna, melakukan pelatihan rutin bagi petugas yang melakukan pengolahan dan pengisian data rekam medis elektronik.

DAFTAR PUSTAKA

- Ardianto, E. T., Sabran, S., & Nurjanah, L. (2024). Analisis Aspek Keamanan Data Pasien dalam Implementasi Rekam Medis Elektronik di Rumah Sakit X. *RAMMIK : Jurnal Rekam Medik Dan Manajemen Informasi Kesehatan Vol.*, 3(2), 18–30.

- Budiman, A., Isa, M., & Soekiswati, S. (2025). Analisis risiko dan tindakan pencegahan kebocoran data rekam medis elektronik pasien di RS P Surakarta. *Ranah Research: Journal of Multidisciplinary Research and Development*, 7(3), 2118–2127.
- M, R. F., Sety, L. O. M., & Hartoyo, A. M. (2024). Jurnal administrasi dan kebijakan kesehatan. *Jurnal Administrasi Dan Kebijakan Kesehatan (Jakk-Uho)*, 5(2), 238–247.
- Nadya Putri Mtd, Muhammad Ikhsan Butarbutar, Sri Apulina Br Sinulingga, Jelita Ramadhani Marpaung, & Rosa Marshanda Harahap. (2023). Pentingnya Evaluasi Dalam Pembelajaran Dan Akibat Memanipulasinya. *Dewantara : Jurnal Pendidikan Sosial Humaniora*, 2(1), 249–261. <https://doi.org/10.30640/dewantara.v2i1.722>
- Pradita, R., Kusumo, R., & Rahmawati. (2022). Pentingnya Aspek Keamanan Informasi Data Pasien Pada Penerapan Rme Di Puskesmas. *Journal of Sustainable Community Service*, 2(2), 52–62. <https://doi.org/10.55047/jscs.v2i2.437>
- Tiorentap, D. R. A., & Hosizah, H. (2020). Aspek Keamanan Informasi dalam Penerapan Rekam Medis Elektronik di Klinik Medical Check-Up MP. *4th Proceeding Perspektif Implementasi FHIR. ISBN: 978-623-6566-34-3*, 4(0), 79–84.
- Ujung, A. M., Irwan, M., & Nasution, P. (2023). Pentingnya Sistem Keamanan Database untuk melindungi data pribadi. *JISKA: Jurnal Sistem Informasi Dan Informatika*, 1(2), 44.
- Vansuri, R., Fauzi, A., Prasetyo, E. T., Negara, R., Ramadhan, R., Restu, A. M., & Firmansyah, R. R. (2023). Peran CIA (Confidentiality, Integrity, Availability) terhadap manajemen keamanan informasi. *Jurnal Ilmu Multidisplin*, 2(1), 106–113.