

Literature Review: Keamanan Data Pasien Rekam Medis Elektronik Berdasarkan ISO27001 Di Fasilitas Kesehatan

Syahfira Nur Jannah¹, Untung Slamet², Achmad Jaelani Rusdi³

^{1,2,3} Program Studi DIII Rekam Medis dan Informasi Kesehatan Institut Teknologi Sains dan Kesehatan RS dr. Soepraoen Kesdam V/BRW Malang

¹shafiraaajhe@gmail.com; ²untungslamet@itsk-soepraoen.ac.id;

³achmadjaelani@itsksoepraoen.ac.id

* corresponding author: shafiraaajhe@gmail.com

Abstrak

Keamanan data pasien dalam rekam medis elektronik (EMR) menjadi perhatian utama di fasilitas kesehatan. Penelitian ini bertujuan untuk menganalisis keamanan data EMR berdasarkan standar ISO 27001 melalui metode kajian pustaka. Data dikumpulkan dari berbagai penelitian sebelumnya yang membahas aspek keamanan informasi dalam penerapan EMR. Hasil penelitian menunjukkan bahwa meskipun mekanisme keamanan seperti autentikasi, enkripsi, dan kontrol akses telah diterapkan, namun masih ditemukan kelemahan dalam pengelolaan hak akses, pencatatan aktivitas pengguna, dan kebijakan keamanan. Beberapa fasilitas kesehatan belum sepenuhnya memenuhi standar ISO 27001, terutama dalam aspek dokumentasi manajemen risiko dan evaluasi keamanan. Oleh karena itu, perlu dilakukan peningkatan kebijakan keamanan, pelatihan tenaga medis, dan pemberian evaluasi berkala untuk memastikan perlindungan data pasien yang lebih baik.

Kata kunci: Fasilitas Kesehatan; Keamanan Data ; Rekam Medis Elektronik; ISO 27001.

Abstract

Patient data security in electronic medical records (EMR) is a major concern in healthcare facilities. This study aims to analyze EMR data security based on the ISO 27001 standard through a literature review method. Data were collected from various previous studies that discussed aspects of information security in the implementation of EMR. The results of the study indicate that although security mechanisms such as authentication, encryption, and access control have been implemented, weaknesses are still found in the management of access rights, recording user activities, and security policies. Several healthcare facilities have not fully met the ISO 27001 standard, especially in the aspects of risk management documentation and security evaluation. Therefore, it is necessary to improve security policies, train medical personnel, and provide periodic evaluations to ensure better protection of patient data.

Keywords: Data Security; Electronic Medical Records; ISO 27001; Healthcare Facilities

PENDAHULUAN

Fasilitas Pelayanan Kesehatan (Fasyenkes) merupakan sarana yang digunakan untuk menyelenggarakan pelayanan kesehatan bagi masyarakat. Fasyankes terdiri dari fasilitas pelayanan kesehatan tingkat pertama, seperti Puskesmas, klinik, dan praktik mandiri tenaga kesehatan, serta fasilitas pelayanan kesehatan rujukan, seperti rumah sakit. Salah satu dokumen yang penting dalam fasilitas kesehatan disebut dengan dokumen Rekam Medis. Berdasarkan Permenkes Nomor 24 Tahun 2022 Rekam Medis adalah dokumen yang

berisikan data identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang telah diberikan kepada pasien.

Seiring perkembangan teknologi dalam berbagai bidang, salah satunya pada bidang kesehatan. Perkembangan signifikan dalam bidang kesehatan mengacu pada penerapan rekam medis elektronik (electronic medical records/ERM). Pemerintah juga telah menetapkan kebijakan wajib penerapan rekam medis elektronik melalui Permenkes Nomor 24 Tahun 2022 .Keamanan dan privasi data pada rekam medis elektronik (RME) menjadi aspek penting dalam menjaga kerahasiaan dan integritas informasi kesehatan pasien. Adopsi RME di seluruh dunia telah mempercepat proses digitalisasi data pasien, meningkatkan efisiensi pelayanan kesehatan (Keshta dan Odeh, 2021). Meskipun penerapan RME telah menjadi kewajiban, masih terdapat tantangan dalam memastikan sistem tersebut sesuai dengan standar keamanan internasional seperti ISO 27001. Standar ini penting untuk menjamin keamanan data pasien, namun praktik di lapangan seringkali belum memadai.

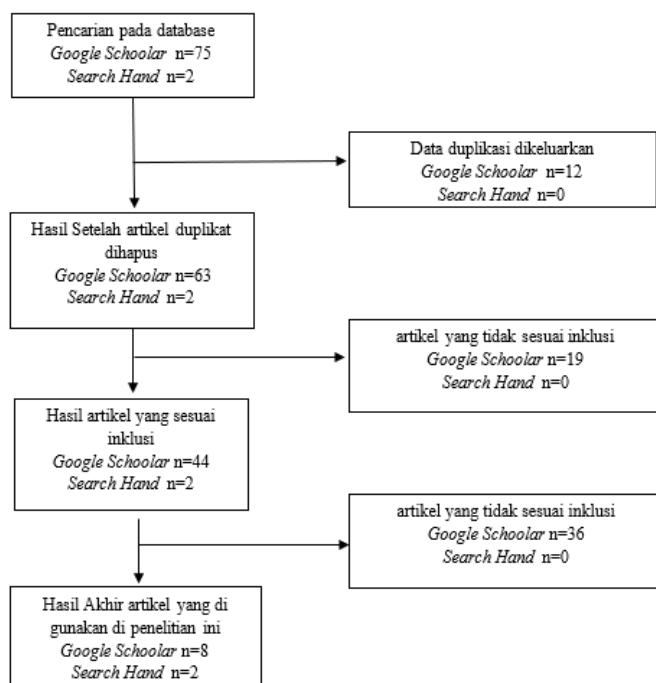
ISO 27001 adalah standar internasional yang dirancang untuk mengelola keamanan informasi di dalam suatu organisasi. Standar ini memberikan panduan dan kerangka dalam kinerja yang lengkap bagi organisasi untuk melindungi informasi sensitif, termasuk data kesehatan, dari berbagai ancaman dan juga resiko keamanan. ISO 27001 adalah persyaratan untuk mendapatkan sertifikat keamanan informasi khususnya di bidang teknologi (aplikasi). Standar keamanan informasi yang menggantikan BS-7799:2 dan diterbitkan pada mutu internasional ISO 27001.

Penelitian sebelumnya menunjukkan bahwa banyak fasilitas belum sepenuhnya memenuhi standar keamanan yang ditetapkan oleh ISO 27001. Misalnya, penelitian oleh Mohammad Iqbal (2021) menunjukkan bahwa sistem keamanan informasi di RSU Arifin Achmad Pekanbaru masih berada dalam kategori "Tidak Layak" dengan skor Indeks Keamanan Informasi (KAMI) yang rendah. Hal ini menunjukkan perlunya evaluasi dan perbaikan dalam pengelolaan keamanan data pasien.

Berdasarkan latar belakang di atas dimana pentingnya menjaga keamanan rekam medis elektronik pada setiap fasilitas kesehatan, maka peneliti tertarik untuk melakukan penelitian dengan judul "Keamanan Data Pasien Rekam Medis Elektronik Berdasarkan ISO27001 Di Fasilitas Kesehatan (literature review)".

METODE

Metode dalam penelitian ini menggunakan literature review. Literature review adalah metode yang bertujuan untuk mengumpulkan dan mengambil inti dari penelitian sebelumnya dan serta menganalisis beberapa overview para ahli yang tertulis dalam teks (Sofia, et, al, 2022). Literature review dilakukan dengan cara menganalisis, menyintesis, meringkas, dan membandingkan hasil-hasil penelitian yang satu dengan lainnya. Data yang digunakan dalam penelitian ini adalah hasil penelitian yang telah dilakukan oleh peneliti terdahulu. Pencarian literature dilakukan pada database online seperti Google Scholar. Pencarian artikel pada database online Google Scholar dengan menggunakan aplikasi Publish or Perish. Artikel yang digunakan adalah artikel yang telah memenuhi kriteria inklusi dan eksklusi, Artikel dapat diakses dan diunduh, Artikel dengan terbitan tahun 2020, 2021, 2022, 2023 dan 2024.



Gambar 1. Pencarian Literature Dan Temuan Artikel

HASIL DAN PEMBAHASAN

Hasil identifikasi artikel yang di temukan pada database google scholar ditemukan 75 artikel sebelum dilakukannya eliminasi sesuai dengan kriteria inklusi dan eksklusi yang telah ditentukan maka diperoleh sebanyak 10 (sepuluh) artikel untuk digunakan. Berikut merupakan hasil temuan artikel ditinjau dari keamanan dan privasi data rekam medis elektronik

Tabel 1. Hasil Temuan Artikel

No	Aspek	Author
1	Keamanan data RME	[1]; [3]; [6]; [7]; [8]; [9]; [10]; [11]; [12]; [3]
2	Privasi data RME	[3], [6], [7], [8], [9]

Berdasarkan tabel 1 menjelaskan bahwa dari temuan 10 artikel didapatkan 10 artikel keamanan data rekam medis elektronik dan 5 artikel privasi data rekam medis elektronik.

1. Keamanan Data Rekam Medis Elektronik di Fasyankes Berdasarkan Standar Keamanan ISO 27001.

Keamanan data pasien dalam implementasi Rekam Medis Elektronik (RME) menjadi perhatian utama dalam berbagai penelitian. Ardianto et al. (2024) menemukan bahwa meskipun sistem login dengan username dan password telah diterapkan di Rumah Sakit X, praktik penggantian password secara berkala dan penggunaan karakter khusus masih kurang diperhatikan. Selain itu, meskipun fitur edit hanya dapat diakses oleh petugas sesuai hak akses, perubahan data harus mengikuti prosedur ketat untuk menjaga integritas. Aspek autentikasi telah diterapkan melalui tanda tangan elektronik, tetapi beberapa formulir masih memerlukan tanda tangan manual. Ketersediaan data terjamin karena akses RME dibatasi hanya di lingkungan rumah sakit, namun semua poli dapat mengakses data pasien, yang berpotensi menimbulkan risiko kebocoran data. Kontrol akses juga diterapkan menggunakan username dan password, tetapi tampilan menu yang sama untuk semua pengguna meningkatkan potensi ancaman keamanan.

Beberapa penelitian lain juga mengungkapkan kelemahan dalam penerapan keamanan informasi RME di rumah sakit dan klinik. Iqbal (2024) mengevaluasi keamanan sistem informasi di RSUD Arifin Achmad Pekanbaru menggunakan ISO 27001 dan menemukan bahwa tingkat kematangan keamanan informasi masih rendah, dengan skor 308 dari 645, yang mengindikasikan status "Tidak Layak". Masalah utama yang diidentifikasi adalah tidak adanya kerangka kerja pengelolaan risiko yang terdokumentasi dan kurangnya tanggung jawab manajemen risiko hingga tingkat pimpinan. Sementara itu, penelitian Maraqqonitilla & Palupi (2024) di RSUD Dr. R. Sosodoro Djatikoesemo Bojonegoro menunjukkan bahwa meskipun kategori sistem elektronik mendapatkan skor tinggi, tata kelola keamanan informasi dan pengelolaan risiko masih memerlukan perhatian lebih. Diperlukan kebijakan yang lebih kuat, peningkatan kesadaran staf, serta evaluasi berkala untuk meningkatkan keamanan informasi rumah sakit.

Selain itu, beberapa studi juga menyoroti pentingnya integritas dan kontrol akses dalam sistem RME. Pramesti et al. (2022) mengungkapkan bahwa meskipun username, password, dan enkripsi data telah diterapkan, tantangan masih muncul dalam menjaga integritas data karena beberapa sistem tidak dapat mencatat perubahan tanpa menghapus informasi sebelumnya. Hal ini berisiko menyebabkan pemalsuan data medis. Selain itu, pengelolaan ID pengguna dan pengawasan kontrol akses masih lemah. Di RSUD Daerah Idaman Banjarbaru, Putri et al. (2024) menemukan bahwa meskipun aspek privasi, integritas, dan autentikasi telah diterapkan, pengelolaan akses pengguna dan fitur seperti automatic log-off masih kurang optimal. Oleh karena itu, evaluasi berkala dan pelatihan staf sangat diperlukan untuk meningkatkan kesadaran dan kepatuhan terhadap prosedur keamanan informasi.

Penelitian lain juga menekankan perlunya kebijakan keamanan yang lebih kuat dan kepatuhan terhadap standar internasional. Rusdiana et al. (2024) menunjukkan bahwa di Rumah Sakit Hermina Serpong, kebijakan keamanan data pasien sudah diterapkan melalui Surat Peraturan Direktur, tetapi implementasinya masih memerlukan peningkatan dalam prosedur operasional standar (SPO) dan pengelolaan akses data. Susanto & Legowo (2023) dalam penelitiannya di laboratorium klinik yang terakreditasi ISO 15189 dan tersertifikasi ISO 9001 menemukan bahwa risiko keamanan informasi tertinggi berasal dari Departemen Business Development & IT, yang memerlukan kontrol tambahan dalam klasifikasi informasi

dan pengelolaan penyedia layanan pemasok. Selain itu, Tiorentap & Hosizah (2020) mencatat bahwa di klinik Medical Check-Up MP, masih ditemukan kelemahan dalam aspek kerahasiaan, integritas, autentikasi, ketersediaan, dan kontrol akses, terutama karena belum dilakukan audit internal maupun eksternal sesuai standar ISO 27001.

Secara keseluruhan, meskipun banyak rumah sakit dan fasilitas kesehatan telah menerapkan langkah-langkah keamanan dalam sistem RME, masih terdapat banyak celah yang perlu diperbaiki. Shovia et al. (2022) mengidentifikasi enam aspek utama dalam keamanan data pasien, yaitu informasi privasi, integritas, autentikasi, ketersediaan, kontrol akses, dan non-repudiation, yang masing-masing masih memiliki tantangan tersendiri. We'e & Siswatibudi (2023) dalam penelitian di Rumah Sakit Panti Nugroho juga menemukan bahwa meskipun sistem keamanan telah berjalan dengan baik, masih ada kendala teknis seperti error sistem dan koneksi internet yang lemah, yang dapat mengganggu aksesibilitas data. Oleh karena itu, perbaikan berkelanjutan dalam kebijakan, prosedur, infrastruktur, dan kesadaran staf sangat diperlukan untuk memastikan perlindungan data pasien yang lebih baik serta kepatuhan terhadap standar keamanan informasi.

2. Privasi Data Rekam Medis Elektronik Di Fasyankes Berdasarkan Standar Keamanan ISO 27001.

Privasi dan perlindungan data rekam medis elektronik di berbagai fasilitas kesehatan telah diterapkan melalui berbagai mekanisme keamanan, seperti autentikasi dengan username dan password, kontrol akses, enkripsi, serta pencatatan aktivitas pengguna. Misalnya, di Rumah Sakit X, sistem keamanan mencakup autentikasi dan tanda tangan elektronik. Namun, masih terdapat kelemahan, seperti belum adanya SOP khusus terkait keamanan data, kurangnya penggantian password secara berkala, serta akses yang tidak terbatas bagi semua poli, sehingga rumah sakit ini belum memenuhi standar keamanan ISO 27001 (Ardianto, et, al, 2024). Hal serupa juga terjadi di fasilitas kesehatan lain yang telah menerapkan autentikasi, enkripsi, dan pembatasan akses, tetapi masih memiliki risiko kebocoran data akibat kurangnya pengawasan, yang membuat penerapannya belum sesuai dengan standar ISO 27001 (Pramesti, et, al., 2022).

Di RS Hermina Serpong, kebijakan dan prosedur keamanan rekam medis elektronik telah cukup lengkap, termasuk penerapan Security Level Group dan penggunaan AWS Cloud untuk melindungi data pasien. Selain itu, rumah sakit ini juga telah memiliki SOP khusus terkait keamanan dan kerahasiaan data medis. Meskipun demikian, tingkat kematangan digitalisasi rumah sakit ini masih berada pada level 2, sehingga belum sepenuhnya sesuai dengan standar ISO 27001 (Rusdiana, et, al., 2024). Sementara itu, beberapa fasilitas kesehatan lain telah menerapkan berbagai langkah keamanan, seperti enkripsi, backup data, serta kontrol akses berbasis username dan password. Namun, kelemahan masih ditemukan dalam pengawasan akses, belum diterapkannya tanda tangan digital di beberapa fasilitas, serta pencatatan perubahan data yang belum optimal, yang mengakibatkan fasilitas tersebut belum memenuhi standar ISO 27001 (Shovia, et, al., 2022).

Di RS Panti Nugroho, sistem keamanan rekam medis elektronik sudah cukup baik dengan penerapan user ID dan password bagi setiap pengguna, hak akses yang dibatasi sesuai jabatan, serta kebijakan keamanan data yang telah diterapkan. Rumah sakit ini juga memiliki sistem kontrol akses dan pencatatan aktivitas pengguna untuk menjaga integritas data. Namun, masih terdapat kendala seperti potensi kebocoran data akibat hak akses yang terlalu luas dan gangguan teknis, sehingga RS Panti Nugroho juga belum sepenuhnya memenuhi standar ISO 27001 (We'e & Siswatibudi, 2023). Secara keseluruhan, meskipun berbagai fasilitas kesehatan telah menerapkan langkah-langkah keamanan data pasien, masih banyak

kendala yang perlu diperbaiki agar dapat sepenuhnya sesuai dengan standar keamanan ISO 27001.

SIMPULAN

Kesimpulan dari penelitian ini, yaitu menunjukkan bahwa penerapan keamanan data pasien dalam Rekam Medis Elektronik (RME) di fasilitas kesehatan masih menghadapi berbagai tantangan, terutama dalam memenuhi standar ISO 27001. Meskipun telah diterapkan mekanisme seperti autentikasi username dan password, enkripsi, serta kontrol akses, masih ditemukan kelemahan dalam aspek pengelolaan hak akses, penggantian password secara berkala, serta pencatatan aktivitas pengguna. Beberapa fasilitas kesehatan belum memiliki SOP khusus terkait keamanan data, sehingga masih terdapat risiko kebocoran informasi pasien.

Selain itu, hasil studi juga menunjukkan bahwa tingkat kematangan keamanan informasi di beberapa rumah sakit masih tergolong rendah. Salah satu penyebab utama adalah kurangnya dokumentasi dalam pengelolaan risiko serta belum optimalnya kebijakan yang mengatur keamanan data pasien. Penerapan standar ISO 27001 masih terbatas pada aspek tertentu, sedangkan aspek lain, seperti audit internal dan evaluasi berkala, masih belum diterapkan secara optimal. Hal ini menunjukkan perlunya peningkatan kesadaran serta komitmen dari pihak manajemen dalam memperkuat sistem keamanan informasi di fasilitas kesehatan.

Secara keseluruhan, meskipun telah ada langkah-langkah untuk meningkatkan keamanan data RME, masih banyak aspek yang perlu diperbaiki agar selaras dengan standar ISO 27001. Implementasi kebijakan yang lebih ketat, pelatihan bagi tenaga medis, serta penggunaan teknologi keamanan yang lebih canggih sangat diperlukan untuk meminimalisir risiko kebocoran data pasien. Dengan demikian, pengelolaan data medis elektronik yang aman dan terpercaya dapat tercapai, serta perlindungan terhadap privasi pasien dapat lebih terjamin.

DAFTAR PUSTAKA

- Ardianto, E. T., Sabran, & 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*, 3(2), 18-30.
- Ikawati, F. R., & Ansyori, A. 2024. A Systematic Review of RME Data Privacy and Security. *Procedia of Engineering and Life Science*, 6, 107-113.

Iqbal, M. (2021). Evaluasi Keamanan Sistem Informasi RSUD Arifin Achmad Pekanbaru Menggunakan ISO 27001. *Tugas Akhir, Universitas Islam Negeri Sultan Syarif Kasim Riau.*

Kementerian Kesehatan Republik Indonesia. Peraturan Menteri Kesehatan Indonesia Nomor 24 Tahun 2022 "Tentang Rekam Medis". Jakarta: Kementerian Kesehatan

Keshta, I., & Odeh, A. 2021. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), 177-183.

Maraqonitatilla, & Palipi, G. S. (2024). Analisis Tingkat Keamanan Informasi Pada RSUD Dr. R. Sosodoro Djatikoesoemo Bojonegoro Menggunakan Indeks KAMI Berdasarkan ISO 27001:2013. *Journal of Emerging Information Systems and Business Intelligence*, 5(2), 66-72. E-ISSN 2774-3993.

PERMENKES 24 TAHUN (2022). "Keamanan dan Perlindungan Data" Pasal 29 Ayat (1)

PERMENKES 24 TAHUN (2022). "Sistem Elektronik dalam Penyelenggaraan Rekam Medis Elektronik" Pasal 10 Ayat (1).

Pramesti, D. P. A., Ayuningtyas, D., & Verdi, R. (2024). Keamanan dan Kerahasiaan Data Medis Pasien dalam Implementasi Rekam Medis Elektronik: Tinjauan Sistematis. PREPOTIF: Jurnal Kesehatan Masyarakat, 8(3), 7691-7702.

Putri, R., Khairunnisa, & Apriyanti, F. (2024). Tinjauan Kesiapan Keamanan Informasi Rekam Medis Elektronik Melalui ISO 27001 Di Instalasi Rawat Jalan Rumah Sakit Daerah Idaman Banjarbaru. Jurnal Kesehatan Indonesia, 10(1), 128-134.

Rusdiana, I., Utama, T., Sucipto, & Muhammad, A. R. (2024). Tinjauan Keamanan dan Kerahasiaan Rekam Medis Elektronik di Rumah Sakit Hermina Serpong. E DU RMIK Journal, 3(2), 1-20.

Sofia, S., Ardianto, E. T., Muna, N., & Sabran, S. 2022. Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Fasilitas Kesehatan. Jurnal Rekam Medik & Manajemen Informasi Kesehatan, 1(2), 94-103.

Susanto, E., & Legowo, N. (2023). Hasil Penilaian Risiko Keamanan Informasi pada Laboratorium Klinik Berdasarkan Kriteria Kendali Dalam Penerapan ISO 27001. Jurnal Rekayasa Sistem Industri, 12(2), 155-164.

Tiorentap, D. R. A., & Hosizah. (2020). Aspek Keamanan Informasi dalam Penerapan Rekam Medis Elektronik di Klinik Medical Check-Up. Prosiding 4 SE NW O D I PA 2020, 53-66. ISBN: 978-623-6566-34-3.

We'e, A., Nugroho, R. H., & Siswatibudi, H. (2023). Evaluasi Aspek Keamanan dan Kerahasiaan Rekam Medis Elektronik di Rumah Sakit Panti Nugroho. Jurnal Permata Indonesia, 14(2), 72-81.