

KEAMANAN DATA PASIEN DALAM REKAM MEDIS ELEKTRONIK ADAPTASI ISO 27001 RUMAH SAKIT NIRMALA PURBALINGGA

Riri Aulia Suprianto^{1*}, Khusnul Khotimah Arum², Ripando Jhon Satria Sembiring³

^{1,2,3}Politeknik Yakpermas Banyumas

¹ririaulia1807@gmail.com, ²arumgusta@gmail.com

³ripandosembiring99@gmail.com

*Corresponding Autor

Informasi Artikel

Pengajuan : 18-08-2026
Ulasan : 24-08-2026
Direvisi : 07-09-2026
Diterima : 14-09-2026
Diterbitkan : 20-09-2026

Kata Kunci:

Human, Kebijakan dan
Prosedur, Keamanan Data
Pasien, Rekam Medis
Elektronik

Abstrak

Penelitian ini bertujuan untuk menggambarkan keamanan data pasien pada penerapan rekam medis elektronik (RME) di RSUD Nirmala Purbalingga dengan menggunakan indikator yang diadaptasi dari ISO 27001:2022. Metode penelitian yang digunakan adalah kuantitatif deskriptif dengan total sampling terhadap 12 responden yang terdiri atas petugas teknologi informasi (IT) dan petugas rekam medis. Pengumpulan data dilakukan pada Mei 2026 menggunakan kuesioner yang terdiri atas 18 item pernyataan dengan skala Likert lima tingkat, yang mencakup tiga aspek keamanan, yaitu human, teknologi, serta kebijakan dan prosedur keamanan. Analisis data dilakukan secara deskriptif menggunakan frekuensi dan persentase berdasarkan kriteria kategorisasi yang ditetapkan secara operasional. Hasil penelitian menunjukkan bahwa seluruh responden (12 orang; 100%) menilai aspek human, teknologi, serta kebijakan dan prosedur keamanan berada dalam kategori diterapkan, sedangkan tidak terdapat responden (0%) yang menilai ketiga aspek tersebut dalam kategori tidak diterapkan. Simpulan penelitian menunjukkan bahwa indikator keamanan data pasien pada RME berdasarkan ketiga aspek yang diteliti dinilai telah diterapkan oleh seluruh responden. Namun, hasil tersebut merupakan gambaran berdasarkan persepsi responden dan belum dapat digunakan untuk menyimpulkan efektivitas seluruh kontrol keamanan maupun tingkat kepatuhan rumah sakit terhadap keseluruhan persyaratan ISO 27001:2022.

How to cite : Suprianto, R. A., Arum, K. K., & Sembiring, R. J. S. (2026). Keamanan Data Pasien Dalam Rekam Medis Elektronik Adaptasi ISO 27001 Rumah Sakit Nirmala Purbalingga. Jurnal Ilmu Kesehatan Masyarakat (JoPHS), 3(3), 523–533. <https://doi.org/10.70248/jophs.v3i3.4448>

DOI : <https://doi.org/10.70248/jophs.v3i3.4448>

Artikel ini merupakan artikel akses terbuka di bawah lisensi <https://creativecommons.org/licenses/by/4.0/>

Hak Cipta© 2026 oleh Penulis. Diterbitkan oleh Yayasan Nuraini Ibrahim Mandiri



PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan dalam berbagai bidang, termasuk pelayanan kesehatan, dari penggunaan sistem konvensional menuju penerapan sistem berbasis digital. Dalam sektor kesehatan, pemanfaatan teknologi informasi berperan dalam menunjang proses pengelolaan pelayanan, mengatur alur kerja, membantu proses pengambilan keputusan, serta mengelola dan menganalisis informasi kesehatan (Melisa et al., 2024). Salah satu implementasi teknologi tersebut adalah rekam medis elektronik (RME), yaitu sistem yang digunakan untuk menyimpan dan mengelola data serta informasi kesehatan pasien dalam bentuk elektronik (Kesuma, 2023). Penerapan RME berperan dalam menunjang pelaksanaan pelayanan kesehatan, tetapi di sisi lain juga menimbulkan potensi risiko keamanan yang dapat berdampak pada integritas dan kerahasiaan informasi pasien (Asih et al., 2024).

Meningkatnya penerapan teknologi digital dalam pelayanan kesehatan turut

meningkatkan potensi terjadinya ancaman terhadap keamanan informasi. Ancaman siber, seperti ransomware dan insiden kebocoran data, berpotensi mengganggu kerahasiaan, integritas, serta ketersediaan informasi kesehatan. Di Amerika Serikat, sebanyak 732 juta rekam medis dilaporkan terdampak insiden keamanan selama periode 2010 sampai 2024, yang menunjukkan bahwa peretasan atau insiden terkait teknologi informasi dan ransomware merupakan bagian dari permasalahan keamanan data kesehatan (Jiang et al., 2025). Kondisi tersebut menegaskan bahwa aspek keamanan informasi perlu diperhatikan dalam pengelolaan sistem digital pada pelayanan kesehatan. Selain itu, laporan mengenai kebocoran data kesehatan di Indonesia turut memperlihatkan bahwa perlindungan terhadap informasi kesehatan pasien merupakan hal yang penting (Nugraha et al., 2025).

Perlindungan keamanan pada rekam medis elektronik (RME) tidak hanya bergantung pada penerapan teknologi untuk mencegah berbagai ancaman, tetapi juga dipengaruhi oleh aspek pengguna, proses kerja, kebijakan, dan prosedur yang mendukung perlindungan informasi. Kerentanan terhadap keamanan informasi dapat dipengaruhi oleh berbagai faktor manusia dan organisasi, antara lain kesalahan pengguna, pengelolaan manajemen, penerapan kebijakan, penggunaan teknologi, serta pelaksanaan pelatihan (Khadka & Ullah, 2025). Penyelenggaraan rekam medis elektronik di Indonesia telah diatur dalam Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang rekam medis. Peraturan tersebut menetapkan bahwa rekam medis elektronik harus memenuhi prinsip keamanan data dan informasi yang meliputi kerahasiaan, integritas, dan ketersediaan (Kementerian kesehatan, 2022). Penerapan ketiga prinsip tersebut menegaskan bahwa keamanan RME mencakup pengelolaan hak akses, pemeliharaan integritas data, dan pemastian ketersediaan informasi sesuai kebutuhan. Kondisi tersebut menunjukkan bahwa pengelolaan keamanan RME membutuhkan pendekatan yang menyeluruh dengan melibatkan aspek human, aspek teknologi, dan kebijakan dan prosedur organisasi.

Keamanan data pasien merupakan salah satu bagian dari keamanan informasi yang bertujuan menjaga kerahasiaan, integritas, dan ketersediaan informasi (Basil et al., 2022). Pada penerapan RME, perlindungan data pasien mencakup pencegahan terhadap akses, pemanfaatan, perubahan, kehilangan maupun pengungkapan informasi oleh pihak yang tidak berwenang (Asih et al., 2024). Dalam penelitian ini, ISO 27001 dijadikan acuan untuk mengidentifikasi dan mengadaptasi indikator keamanan informasi, bukan sebagai standar untuk melakukan audit atau menilai tingkat kepatuhan rumah sakit secara keseluruhan. ISO 27001:2022 menyediakan kerangka sistematis untuk pengelolaan keamanan informasi dan pengendalian risiko, dengan pengendalian yang mencakup aspek organisasional, manusia, dan teknologi (Culot et al., 2021). Kontrol yang relevan dari ISO 27001:2022 disesuaikan menjadi indikator keamanan data pasien pada RME berdasarkan aspek human, teknologi, serta kebijakan dan prosedur. Keamanan informasi dalam penerapannya turut dipengaruhi oleh faktor manusia dan organisasi, termasuk perilaku, proses pengambilan keputusan, serta budaya organisasi, selain aspek teknologi (Khadka & Ullah, 2025).

Berdasarkan hasil observasi awal di RSUD Nirmala Purbalingga, sistem rekam medis elektronik (RME) telah diterapkan dalam pelayanan kesehatan. Dalam penerapannya, sistem menggunakan login dengan username dan password, pembatasan hak akses pengguna, serta kebijakan kerahasiaan data pasien. Meskipun demikian, keberadaan mekanisme tersebut belum dapat memastikan bahwa pengelolaan keamanan informasi telah berjalan secara optimal. Oleh karena itu, diperlukan peninjauan terhadap keamanan data pasien dalam RME dengan

mempertimbangkan aspek human, teknologi, serta kebijakan dan prosedur keamanan informasi. Penelitian terdahulu menunjukkan bahwa perlindungan data dalam RME dapat diperkuat melalui autentikasi pengguna, log out otomatis, pembaruan password secara berkala, dan pengendalian akses (Sari Chintia et al., 2021). Namun, penerapannya tetap memiliki risiko yang dipengaruhi oleh faktor pengguna dan organisasi, salah satunya penggunaan user ID milik petugas lain (Melisa et al., 2024). Oleh karena itu, keamanan RME perlu ditinjau dengan mempertimbangkan aspek human, teknologi, dan organisasi.

Penelitian terdahulu telah membahas keamanan RME dari aspek teknologi, pengguna, pengendalian akses, dan organisasi. Namun, studi mengenai keamanan data pasien secara terintegrasi menggunakan indikator yang diadaptasi dari ISO 27001, meliputi aspek human, teknologi, serta kebijakan dan prosedur, masih terbatas pada penerapan RME di RSUD Nirmala Purbalingga. Oleh karena itu, penelitian ini dilakukan untuk meninjau keamanan data pasien dalam RME menggunakan indikator yang terstruktur dan disesuaikan dengan penerapan RME di rumah sakit. Penelitian ini memberikan kontribusi melalui penggunaan indikator yang diadaptasi dari ISO 27001 untuk meninjau keamanan data pasien pada RME berdasarkan tiga aspek, yaitu human, teknologi, serta kebijakan dan prosedur keamanan informasi di RSUD Nirmala Purbalingga. Pendekatan ini diharapkan dapat memberikan gambaran yang lebih sistematis mengenai penerapan keamanan data pasien dalam pengelolaan RME. Penelitian ini bertujuan untuk menggambarkan kondisi keamanan data pasien pada penerapan rekam medis elektronik (RME) di RSUD Nirmala Purbalingga dengan menggunakan indikator yang diadaptasi dari ISO 27001.

METODE PENELITIAN

Penelitian ini menggunakan metode kuantitatif deskriptif untuk memperoleh gambaran mengenai keamanan data pasien pada sistem rekam medis elektronik melalui indikator yang disusun berdasarkan adaptasi dari kontrol ISO 27001:2022 yang relevan. ISO 27001:2022 dimanfaatkan sebagai landasan dalam menentukan dan menyesuaikan indikator keamanan informasi yang relevan, bukan untuk melakukan audit maupun mengukur kepatuhan rumah sakit terhadap keseluruhan persyaratan standar (ISO 27001, 2022). Penelitian ini dilaksanakan di Rumah Sakit Umum Nirmala Purbalingga. Populasi penelitian mencakup seluruh petugas yang berperan dalam pengelolaan sistem rekam medis elektronik di RSUD Nirmala Purbalingga, meliputi petugas teknologi informasi (IT) dan petugas rekam medis. Penentuan sampel menggunakan teknik total sampling, sehingga seluruh anggota populasi yang memenuhi kriteria penelitian ditetapkan sebagai responden. Jumlah responden dalam penelitian ini adalah 12 orang yang terdiri atas petugas IT dan petugas rekam medis. Pengumpulan data dilakukan pada Mei 2026.

Instrumen penelitian disusun berdasarkan adaptasi terhadap kontrol keamanan informasi yang relevan dalam ISO 27001:2022 dan disesuaikan dengan penerapan keamanan data pasien pada sistem rekam medis elektronik. Kontrol tersebut kemudian dioperasionalkan menjadi indikator penelitian yang mencakup tiga aspek, yaitu human, teknologi, serta kebijakan dan prosedur keamanan. Instrumen terdiri atas 18 item pernyataan, yaitu 6 item aspek human, 6 item aspek teknologi, dan 6 item aspek kebijakan dan prosedur keamanan. Pengukuran setiap item menggunakan skala likert lima tingkat, yaitu sangat tidak setuju (skor 1), tidak setuju (skor 2), netral (skor 3), setuju (skor 4) dan sangat setuju (skor 5). Keterkaitan antara kontrol ISO 27001:2022, indikator, item pernyataan, metode pengukuran, dan hasil penelitian disajikan dalam

matriks operasionalisasi instrumen.

Tabel 1.

Matriks Adaptasi Indikator Keamanan Data Pasien dalam Rekam Medis Elektronik Berdasarkan ISO 27001:2022

Dasar ISO 27001;2022	Indikator	Item Pernyataan	Pengukuran	Hasil Pengukuran
A.6.3	Kesadaran keamanan informasi	Saya memahami pentingnya kerahasiaan data pasien dalam RME	Likert 1-5	Diterapkan
A.6.3	Pelatihan keamanan informasi	Saya pernah mendapatkan pelatihan tentang keamanan informasi	Likert 1-5	Diterapkan
A.5.17	Informasi autentikasi	Saya menggunakan password pribadi dan tidak membagikannya kepada orang lain	Likert 1-5	Diterapkan
A.8.5	Perilaku logout pengguna	Saya selalu logout setelah selesai menggunakan sistem	Likert 1-5	Diterapkan
A.6.8	Pelaporan kejadian keamanan informasi	Saya mengetahui prosedur pelaporan jika terjadi insiden keamanan	Likert 1-5	Diterapkan
A.6.4	Proses disipliner	Terdapat sanksi bagi pelanggaran keamanan data	Likert 1-5	Diterapkan
A.8.5	Autentikasi pengguna	Sistem rekam medis menggunakan username dan password unik untuk setiap pengguna	Likert 1-5	Diterapkan
A.8.3	Pembatasan hak akses	Sistem memiliki pembatasan hak akses sesuai jabatan	Likert 1-5	Diterapkan
A.8.24	Kriptografi/ enkripsi	Data pasien dilindungi dengan sistem enkripsi	Likert 1-5	Diterapkan
A.8.13	Pencadangan informasi	Sistem memiliki fitur backup data secara berkala	Likert 1-5	Diterapkan
A.8.7	Perlindungan terhadap malware	Sistem memiliki antivirus atau proteksi malware	Likert 1-5	Diterapkan
A.8.5	Automatic logout	Sistem secara otomatis logout jika tidak digunakan dalam waktu tertentu	Likert 1-5	Diterapkan
A.5.1	Kebijakan keamanan informasi	Rumah sakit memiliki kebijakan tertulis tentang keamanan informasi	Likert 1-5	Diterapkan
A.5.37	Prosedur operasional	Terdapat SOP penggunaan sistem rekam medis elektronik	Likert 1-5	Diterapkan
A.5.24	Pelaporan insiden	Terdapat prosedur pelaporan insiden keamanan data	Likert 1-5	Diterapkan
Klausul 9.1	Evaluasi keamanan informasi	Rumah sakit melakukan evaluasi keamanan secara berkala	Likert 1-5	Diterapkan
Klausul 9.2	Audit/ peninjauan keamanan	Terdapat audit internal terkait keamanan informasi	Likert 1-5	Diterapkan
A.5.31	Kepatuhan terhadap regulasi	Rumah sakit mematuhi regulasi perlindungan data pasien	Likert 1-5	Diterapkan

Hasil uji validitas menunjukkan seluruh item pada aspek human, teknologi, serta kebijakan dan prosedur keamanan dinyatakan valid. Uji reliabilitas dilakukan menggunakan metode *Cronbach's Alpha*. Hasil uji reliabilitas menunjukkan nilai Cronbach's Alpha masing-masing sebesar 0,886, 0,885, dan 0,878, sehingga instrument pada ketiga aspek dinyatakan reliabel. Pengumpulan data dilakukan dengan memberikan kuesioner kepada 12 responden yang terdiri atas petugas teknologi

informasi (IT) dan petugas rekam medis di RSUD Nirmala Purbalingga. Analisis data dilakukan secara kuantitatif deskriptif dengan memberikan skor terhadap setiap jawaban pada item pernyataan kuesioner. Perolehan skor selanjutnya dihitung dan dikelompokkan berdasarkan tiga aspek yang diteliti, yaitu human, teknologi, serta kebijakan dan prosedur keamanan. Hasil analisis kemudian disajikan dalam bentuk frekuensi dan persentase untuk memberikan gambaran mengenai penerapan keamanan data pasien pada sistem rekam medis elektronik. Penentuan kategori dilakukan berdasarkan nilai tengah dari rentang skor skala likert. Setiap aspek terdiri atas enam item pernyataan dengan rentang skor 1-5, sehingga skor minimum setiap aspek adalah 6 dan skor maksimum adalah 30. Nilai tengah skala diperoleh dengan rumus $(\text{skor minimum} + \text{skor maksimum})/2$, yaitu $(6+30)/2 = 18$. Selanjutnya, nilai 18 digunakan sebagai batas kategorisasi. Skor <18 dikategorikan sebagai tidak diterapkan, sedangkan skor ≥ 18 dikategorikan sebagai diterapkan. Batas kategorisasi tersebut ditetapkan sebagai kriteria operasional dalam penelitian dan bukan merupakan ketentuan cut-off yang ditetapkan oleh ISO 27001:2022.

HASIL PENELITIAN DAN PEMBAHASAN

Tabel 2.

Hasil Penilaian Keamanan Data Pasien pada Rekam Medis Elektronik Berdasarkan Aspek Human, Teknologi, serta Kebijakan dan Prosedur Keamanan

No	Aspek	Jumlah Responden	Diterapkan (f)	Diterapkan (%)	Tidak diterapkan (f)	Tidak diterapkan (%)
1.	Human	12	12	100%	0	0%
2.	Teknologi	12	12	100%	0	0%
3.	Kebijakan dan prosedur keamanan	12	12	100%	0	0%

Hasil penelitian menunjukkan bahwa sebanyak 12 responden (100%) menilai ketiga aspek keamanan data pasien, yaitu aspek human, teknologi, serta kebijakan dan prosedur keamanan, berada dalam kategori diterapkan. Tidak terdapat responden yang memberikan penilaian pada kategori tidak diterapkan. Berdasarkan penilaian responden dan kriteria kategorisasi yang digunakan, ketiga aspek keamanan data pasien termasuk dalam kategorisasi diterapkan.

Hasil penilaian sebesar 100% pada seluruh aspek perlu dimaknai secara cermat agar tidak menimbulkan kesimpulan yang berlebihan. Persentase tersebut belum dapat dijadikan bukti bahwa keamanan data pasien telah diterapkan secara keseluruhan maupun bahwa setiap kontrol telah berjalan efektif, karena hasil penelitian didasarkan pada persepsi responden. Hasil 100% pada seluruh aspek juga dapat dipengaruhi oleh *social desirability bias*, yaitu kecenderungan responden memberikan jawaban yang dianggap sesuai dengan harapan organisasi. Dalam penelitian ini, skor 18 digunakan sebagai batas kategorisasi yang diperoleh dan nilai tengah rentang skor 6-30 dan ditetapkan sebagai kriteria operasional, bukan sebagai cut-off berdasarkan ISO 27001. Kondisi tersebut memungkinkan responden yang memiliki tingkat penerapan kontrol yang berbeda tetap diklasifikasikan ke dalam kategori diterapkan yang sama. Oleh sebab itu, hasil kategorisasi yang diperoleh belum mampu menunjukkan perbedaan tingkat kematangan keamanan secara lebih mendalam.

Nilai 100% yang diperoleh belum dapat menunjukkan bahwa seluruh kontrol keamanan telah dilaksanakan secara konsisten, melalui proses verifikasi, serta mampu

berfungsi secara efektif dalam mengurangi risiko keamanan. Hal ini disebabkan penelitian belum melakukan pemeriksaan terhadap objektif, seperti audit log, kepatuhan petugas terhadap SOP, pengujian proses pemulihan data dari backup, maupun verifikasi teknis lainnya. Dengan demikian, hasil 100% lebih tepat dimaknai sebagai gambaran penilaian responden terhadap penerapan indikator keamanan yang diteliti dan belum dapat digunakan untuk menyatakan bahwa seluruh risiko maupun potensi kelemahan keamanan data pasien telah dapat dikendalikan sepenuhnya.

Keamanan Data Pasien Berdasarkan Aspek Human

Berdasarkan penilaian terhadap aspek human dalam keamanan data pasien pada sistem rekam medis elektronik di RSUD Nirmala Purbalingga, seluruh responden yang berjumlah 12 orang (100%) menempatkan aspek human pada kategori diterapkan. Tidak terdapat responden yang menilai aspek tersebut dalam kategori tidak diterapkan. Penilaian positif dari seluruh responden mencakup beberapa indikator, yaitu kesadaran terhadap keamanan informasi, pelatihan keamanan informasi, penggunaan password secara pribadi, pelaksanaan logout setelah menggunakan sistem, pemahaman mengenai prosedur pelaporan insiden, serta penerapan sanksi terhadap pelanggaran keamanan data. Hasil penilaian menunjukkan bahwa kontrol keamanan yang melibatkan pengguna telah diterapkan sebagai bagian dari upaya perlindungan data pasien. Menurut (Culot et al., 2021), keberhasilan pengelolaan keamanan informasi tidak hanya dipengaruhi oleh aspek teknis, tetapi juga oleh faktor organisasi dan budaya keamanan. Perlindungan data pasien dapat diperkuat melalui peningkatan kesadaran keamanan informasi dan evaluasi keamanan yang dilakukan secara rutin (Jannah et al., 2025). Sementara itu, (Hisyam Fadhil & Rojabi Afdan, 2025) menjelaskan bahwa pelatihan keamanan informasi dapat meningkatkan pemahaman dan kepatuhan pengguna terhadap prosedur keamanan. Dengan demikian, berdasarkan persepsi responden, terdapat penerapan kesadaran dan perilaku keamanan yang dapat mendukung upaya perlindungan data pasien.

Meskipun seluruh responden memberikan penilaian positif pada aspek human, hasil tersebut belum menunjukkan bahwa seluruh risiko faktor manusia telah terkendali. Penilaian yang diperoleh hanya menggambarkan persepsi responden terhadap penerapan kontrol dan belum mengukur secara langsung human error, penyalahgunaan hak akses, maupun ketidakpatuhan terhadap prosedur. Peningkatan kesadaran keamanan informasi dapat membantu mengurangi risiko kebocoran data akibat faktor manusia (Rijal et al., 2024), sedangkan edukasi dan pelatihan dapat mendukung pengurangan kesalahan manusia dalam pengelolaan informasi (Ipungkarti Aprila, 2023). Efektivitasnya tetap memerlukan evaluasi terhadap perilaku dan kepatuhan pengguna. Dengan demikian, penerapan kontrol pada aspek human dalam penelitian ini menunjukkan bahwa kontrol terkait kesadaran, pelatihan, dan perilaku keamanan dinilai telah diterapkan oleh responden. Namun, efektivitasnya belum dapat dipastikan hanya melalui kuesioner. Verifikasi melalui observasi perilaku, pemeriksaan kepatuhan, evaluasi pelatihan, atau pencatatan insiden diperlukan untuk memperoleh gambaran yang lebih objektif.

Keamanan Data Pasien Berdasarkan Aspek Teknologi

Berdasarkan penilaian terhadap aspek teknologi dalam keamanan data pasien pada sistem rekam medis elektronik di RSUD Nirmala Purbalingga, seluruh responden yang berjumlah 12 orang (100%) menempatkan aspek teknologi pada kategori diterapkan. Tidak terdapat responden yang menilai aspek tersebut dalam kategori

tidak diterapkan. Penilaian tersebut mencakup penerapan kontrol teknologi berupa penggunaan username dan password unik, pembatasan hak akses berdasarkan jabatan, enkripsi data, pencadangan data secara berkala, perlindungan terhadap malware, serta fitur automatic logout. Autentikasi pengguna, pembatasan hak akses, automatic logout, dan backup dapat mendukung perlindungan keamanan data pada sistem rekam medis elektronik. (Palupi et al., 2026) menunjukkan bahwa penggunaan username dan password pribadi, pembatasan akses, automatic logout, serta backup merupakan bagian dari upaya pengamanan data. Kontrol tersebut, termasuk enkripsi, juga dapat mendukung terjaganya kerahasiaan, integritas, dan ketersediaan data. Namun, keberadaan kontrol teknologi belum menjamin efektivitas pengendaliannya. Username dan password menunjukkan adanya autentikasi, tetapi belum memastikan keamanan password dan peninjauan akun secara berkala. Pembatasan hak akses juga belum membuktikan bahwa kewenangan pengguna diperbarui sesuai perubahan tugas, sedangkan automatic logout hanya merupakan salah satu mekanisme pengamanan sesi. Hal ini sejalan dengan (Pramesti et al., 2024) bahwa kontrol autentikasi, enkripsi, dan pembatasan akses masih dapat menghadapi risiko apabila pengawasan belum optimal.

Penerapan backup data dapat membantu mengurangi risiko kehilangan data, tetapi hasil kuesioner belum dapat memastikan bahwa proses pemulihan data telah diuji atau berjalan efektif ketika terjadi gangguan. Begitu pula, penggunaan enkripsi dan perlindungan terhadap malware belum cukup untuk memastikan efektivitas pengamanan tanpa verifikasi teknis lebih lanjut. Hal ini sejalan dengan (Pramesti et al., 2024) yang menunjukkan bahwa penerapan kontrol keamanan masih dapat menghadapi risiko apabila pengawasan belum optimal. Dengan demikian, hasil 100% pada aspek teknologi menunjukkan bahwa kontrol yang dinilai telah dipersepsikan diterapkan oleh seluruh responden, tetapi belum membuktikan efektivitasnya dalam mengendalikan seluruh risiko keamanan. Temuan ini menunjukkan adanya mekanisme dasar pengamanan teknologi, sedangkan efektivitas kontrol masih memerlukan verifikasi melalui pemeriksaan konfigurasi, audit log, peninjauan hak akses, pengujian pemulihan backup, dan evaluasi keamanan secara berkala.

Keamanan Data Pasien Berdasarkan Aspek Kebijakan dan Prosedur Keamanan

Berdasarkan penilaian terhadap aspek kebijakan dan prosedur keamanan dalam keamanan data pasien pada sistem rekam medis elektronik di RSUD Nirmala Purbalingga, seluruh responden yang berjumlah 12 orang (100%) menempatkan aspek kebijakan dan prosedur keamanan pada kategori diterapkan. Tidak terdapat responden yang menilai aspek tersebut dalam kategori tidak diterapkan. Penilaian positif tersebut mencakup kebijakan tertulis keamanan informasi, SOP penggunaan sistem rekam medis elektronik, prosedur pelaporan insiden, evaluasi keamanan berkala, audit internal, serta kepatuhan terhadap regulasi perlindungan data pasien. Kebijakan dan SOP berperan sebagai pedoman bagi petugas dalam menjalankan pengelolaan serta perlindungan informasi pasien. Penerapan rekam medis elektronik perlu didukung oleh kebijakan dan SOP yang mengatur penggunaan sistem serta hak akses sesuai kewenangan petugas (Rusdi et al., 2024). Selain itu, kebijakan tertulis dan SOP juga menjadi unsur penting dalam menjaga keamanan dan kerahasiaan data pasien (Rusdiana et al., 2026). Adanya kebijakan dan SOP tidak secara langsung membuktikan bahwa pengelolaan risiko keamanan informasi telah berlangsung efektif. Kuesioner yang digunakan belum dapat menggambarkan kepatuhan petugas terhadap SOP, pembaruan dokumen, pelaksanaan audit, tindak lanjut evaluasi, maupun penerapan prosedur saat terjadi insiden keamanan.

Oleh karena itu, hasil 100% pada aspek kebijakan dan prosedur lebih tepat dipahami, sebagai penilaian responden terhadap penerapan kontrol yang diteliti, bukan sebagai bukti bahwa seluruh kebijakan dan SOP telah diterapkan efektif. Berdasarkan penilaian responden, kebijakan dan prosedur dinilai telah diterapkan sebagai bagian dari upaya mendukung keamanan data pasien. Namun, efektivitas penerapannya masih perlu dibuktikan melalui pemeriksaan dokumen, pembaruan SOP, bukti sosialisasi, hasil audit, catatan insiden, dan tindak lanjut evaluasi keamanan. Dengan demikian, penerapan kontrol kebijakan dan prosedur telah teridentifikasi berdasarkan penilaian responden, sedangkan konsistensi dan efektivitas pelaksanaannya memerlukan verifikasi lebih lanjut. Penelitian ini memiliki keterbatasan pada jumlah responden yang hanya 12 orang dan lokasi penelitian yang dilakukan pada satu rumah sakit, sehingga hasil penelitian belum dapat digeneralisasikan ke rumah sakit lain. Selain itu, penggunaan kuesioner membuat hasil penelitian masih bergantung pada persepsi responden dan belum sepenuhnya menggambarkan kondisi keamanan secara objektif. Penelitian selanjutnya dapat melibatkan responden dan lokasi yang lebih beragam serta menggunakan observasi, pemeriksaan dokumen, audit log, dan verifikasi teknis untuk memperoleh hasil yang lebih komprehensif.

KESIMPULAN

Berdasarkan hasil penelitian terhadap 12 responden, penerapan indikator keamanan data pasien dalam sistem rekam medis elektronik yang ditinjau melalui aspek human, teknologi, serta kebijakan dan prosedur keamanan menunjukkan kategori diterapkan. Temuan ini menggambarkan kondisi penerapan indikator yang dinilai berdasarkan jawaban responden, sehingga belum dapat digunakan untuk menyimpulkan tingkat kepatuhan rumah sakit terhadap keseluruhan standar ISO 27001. Untuk mendukung keberlanjutan keamanan data pasien, diperlukan kegiatan audit, pemantauan, dan evaluasi secara berkala serta peningkatan terhadap kontrol keamanan yang telah diterapkan.

Pernyataan tentang Penggunaan Kecerdasan Buatan.

AI digunakan dalam penyusunan manuskrip ini. Para penulis menggunakan alat kecerdasan buatan semata-mata untuk membantu perbaikan bahasa, pengecekan tata bahasa, dan penyuntingan agar lebih jelas dan mudah dibaca. Para penulis tetap bertanggung jawab penuh atas keakuratan, orisinalitas, integritas, dan isi akademis manuskrip. Semua konten yang dibantu AI telah ditinjau dan diverifikasi oleh para penulis sebelum pengajuan.

Konflik Kepentingan

Para penulis menyatakan tidak ada konflik kepentingan

Kontribusi Penelitian

Konseptualisasi, penulis 1, penulis 2, dan penulis 3; pengumpulan data, penulis 1; validasi data, penulis 1 dan penulis 2; analisis formal, penulis 1 dan penulis 2; penulisan-penyusunan draf asli, penulis 1; penulisan-peninjauan dan penyuntingan, penulis 1 dan penulis 3; visualisasi, penulis 1. Semua penulis telah membaca dan menyetujui versi akhir manuskrip.

Ucapan Terima Kasih

Penulis menyampaikan terima kasih kepada RSUD Nirmala Purbalingga yang telah memberikan izin serta menyediakan dukungan, fasilitas, dan akses yang dibutuhkan

selama pelaksanaan penelitian. Terima kasih juga disampaikan kepada pihak manajemen dan seluruh pihak yang terlibat atas kerja sama dan kontribusinya dalam mendukung kelancaran hingga selesainya penelitian ini.

DAFTAR PUSTAKA

- Asih, H. A., Indrayadi, I., Soraya, S., & Khairunnisa, K. (2024). Evaluasi Keamanan Data Pasien Pada Rekam Medis Elektronik Dengan Systematic Literature Review. *Jurnal Ilmiah FIFO*, 16(2), 104. <https://doi.org/10.22441/fifo.2024.v16i2.001>
- Basil, N. N., Ambe, S., Ekhatior, C., & Fonkem, E. (2022). Health Records Database and Inherent Security Concerns: A Review of the Literature. *Cureus*. <https://doi.org/10.7759/cureus.30168>
- Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. In *TQM Journal* (Vol. 33, Number 7, pp. 76–105). Emerald Group Holdings Ltd. <https://doi.org/10.1108/TQM-09-2020-0202>
- Hisyam Fadhil, G., & Rojabi Afdan, M. (2025). Analisis Dan Penerapan Sistem Manajemen Keamanan Aplikasi Point Of Sales Menggunakan ISO 27001. *Integrative Perspectives of Social and Science Journal (IPSSJ)*, 2(1), 1087–1094.
- Ipungkarti Aprila, A. (2023). 2023 Penerapan IT Security Awareness Standar Keamanan ISO 27001 Di BPJS Ketenagakerjaan Kantor Cabang Purwakarta. In *Jurnal Media Infotama* (Vol. 19, Number 1).
- ISO 27001 (2022). <https://www.iso.org/standard/27001>
- Jannah, S. N., Slamet, U., & Rusdi, A. J. (2025). Literature Review: Keamanan Data Pasien Rekam Medis Elektronik Berdasarkan ISO27001 Di Fasilitas Kesehatan.
- Jiang, J. X., Ross, J. S., & Bai, G. (2025). Ransomware Attacks and Data Breaches in US Health Care Systems. *JAMA Network Open*, 8(5), 1–4. <https://doi.org/10.1001/jamanetworkopen.2025.10180>
- Kesuma, S. I. (2023). Rekam Medis Elektronik Pada Pelayanan Rumah Sakit Di Indonesia: Aspek Hukum Dan Implementasi. *Aladalah: Jurnal Politik, Sosial, Hukum Dan Humaniora*, 1(1), 195–205.
- Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. *International Journal of Information Security*, 24(3). <https://doi.org/10.1007/s10207-025-01032-0>
- Melisa, N. P., Sukmaningsih, W. R., & Licia, R. (2024). Analisis Rekam Medis Elektronik Rawat Jalan Pada Aspek Keamanan Data Pasien Di Rumah Sakit Umum Daerah Dr. Soediran Mangun Sumarso Wonogiri. In *JHIMI Journal* (Vol. 03, Number 03).
- Nugraha, D. A., Nurfitroh, R., Ul-Haq, N. D., Dika, R. P., & Lagontang, S. N. (2025). KEBOCORAN DATA BPJS KESEHATAN: ANCAMAN TERHADAP KEAMANAN INFORMASI PUBLIK DI ERA DIGITAL. *Integrative Perspectives of Social and Science Journal*, 2(3), 4685.
- Palupi, D. C., Rahmansyah, I., & Arum, K. K. (2026). Evaluasi Keamanan Data Dalam Sistem Rekam Medis Elektronik Di Rumah Sakit Umum Daerah Banyumas. *RAMMIK : Jurnal Rekam Medis Dan Manajemen Informasi Kesehatan*, 5(1), 1–8. <https://doi.org/10.47134/rmik.v5i1.1897>
- Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 Tentang Rekam Medis (2022). www.Peraturan.Go.Id
- 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.

- Rijal, M. D., Assydiqi, M. F., Prasetya, Y. R., Prasetya Ningsih, L. N., Putri Anindra, N. K., & Pambudi, P. D. L. (2024). Information Security Awareness Analysis of the Threat of Data Leakage in Educational Institutions with the ISO 27001 Framework. *Journal of Digital Business and Innovation Management*, 3(1), 36–52. <https://doi.org/10.26740/jdbim.v3i1.59167>
- Rusdi, A. J., Rusfadir, A., & Raharusun, K. A. A. (2024). Optimalisasi Penerapan Rekam Medis Elektronik di RSUD Karel Sadsitubun Langgur Maluku Tenggara. *ULIL ALBAB : Jurnal Ilmiah Multidisiplin*, 3(8), 773–781.
- Rusdiana, I., Aryani, S. D., Kuntoadi, G. B., Widya Dharma Husada Tangerang, Stik., Pajajaran No, J., Barat, P., & Pamulang, K. (2026). Tinjauan Keamanan Dan Kerahasiaan Data Pasien Terkait Aspek Hukum Rekam Medis Di Rumah Sakit An-Nisa Tangerang. In *Edu Rmik Jurnal Edukasi Rekam Medis Informasi Kesehatan* (Vol. 5, Number 1). <https://openjournal.wdh.ac.id/index.php/MRHI/index>
- Sari Chintia, I., Alvionita Vicky, C., & Gunawan. (2021). Literature Review Analisis Permasalahan Privasi Pada Rekam Medis Elektronik. *Jurnal Rekam Medis Dan Informasi Kesehatan Indonesia (Jurmiki)*, 01(01), 45–52.