Full Paper

Analisis Keamanan Data Pasien pada Sistem Informasi Manajemen Rumah Sakit (SIMRS)

Maradona Jonas Simanullang[1*], Mhd Adi Setiawan Aritonang[2], Frans Mikael Sinaga[3*]
[1]Program Studi Teknologi Informasi, Universitas Senior Medan, Indonesia
[2]Program Studi Teknik Komputer, Institut Teknologi Batam, Indonesia
[3]Faculty of AI and Data Sciences-Informatics Department, Universitas Pelita Harapan, Indonesia

Informasi Artikel

Terbit: Januari 2026

Kata Kunci:

Data Pasien
Keamanan Data
Rumah Sakit
SIMRS
Sistem Informasi Kesehatan

ABSTRAK

Penerapan Sistem Informasi Manajemen Rumah Sakit (SIMRS) berperan penting dalam pengelolaan data pasien yang bersifat sensitif dan membutuhkan tingkat keamanan yang tinggi. Penelitian ini bertujuan untuk menganalisis keamanan data pasien pada SIMRS berdasarkan hasil evaluasi grafik yang mengacu pada prinsip *confidentiality*, *integrity*, dan *availability* (CIA). Metode penelitian yang digunakan adalah studi kasus dengan pendekatan deskriptif, melalui observasi sistem, wawancara dengan tim teknologi informasi, serta analisis kebijakan keamanan informasi. Hasil analisis grafik menunjukkan bahwa aspek *availability* memperoleh skor tertinggi sebesar 4,2, yang mengindikasikan bahwa ketersediaan sistem dan kontinuitas layanan SIMRS telah berjalan dengan baik. Namun, aspek *confidentiality* dan *integrity* masing-masing memperoleh skor 3,5 dan 3,4, yang menunjukkan bahwa perlindungan kerahasiaan dan keutuhan data pasien masih berada pada kategori cukup. Temuan ini mengindikasikan adanya kelemahan pada pengelolaan hak akses, penerapan enkripsi data, serta mekanisme audit aktivitas pengguna. Berdasarkan hasil tersebut, penelitian ini merekomendasikan penguatan kebijakan keamanan informasi, peningkatan kontrol akses dan perlindungan data, serta pengembangan kompetensi sumber daya manusia untuk meningkatkan keamanan data pasien pada SIMRS secara berkelanjutan.

Corresponding Author:

Maradona Jonas Simanullang,
Email: maradonajonassimanullang@gmail.com

1. PENDAHULUAN

Isu keamanan data medis menjadi perhatian yang sangat krusial dalam era transformasi digital layanan kesehatan, mengingat data pasien bersifat sangat sensitif dan bernilai tinggi. Data tersebut tidak hanya mencakup identitas pribadi, tetapi juga informasi klinis yang apabila bocor dapat menimbulkan dampak serius terhadap privasi pasien, keselamatan layanan, serta kepercayaan publik terhadap institusi kesehatan [2], [8]. Dalam beberapa tahun terakhir, rumah sakit menjadi salah satu target utama serangan siber, khususnya serangan ransomware, yang berpotensi melumpuhkan Sistem Informasi Manajemen Rumah Sakit (SIMRS) dan menghambat operasional layanan kesehatan secara signifikan [7], [8], [11]. Berbagai kajian terdahulu terkait keamanan SIMRS umumnya berfokus pada evaluasi teknis sistem, seperti audit keamanan berbasis standar ISO/IEC 27001, COBIT, atau kerangka manajemen risiko tertentu [5], [9], [12]. Meskipun kajian-kajian tersebut memberikan kontribusi penting dalam mengukur tingkat kepatuhan sistem terhadap standar keamanan informasi, sebagian besar penelitian masih terbatas pada aspek teknis dan belum sepenuhnya menggambarkan implementasi keamanan SIMRS dalam praktik operasional rumah sakit [4], [13]. Akibatnya, masih terdapat celah penelitian dalam memahami bagaimana kebijakan keamanan, prosedur kerja, serta interaksi pengguna memengaruhi tingkat keamanan data pasien secara nyata.

Selain itu, beberapa penelitian sebelumnya cenderung menggunakan pendekatan kuantitatif atau audit formal yang menitikberatkan pada pengukuran tingkat risiko atau kepatuhan sistem [5], [12]. Pendekatan tersebut dinilai kurang mampu menangkap permasalahan keamanan yang bersifat kontekstual dan non-teknis, seperti penggunaan akun bersama, lemahnya pengawasan hak akses, serta rendahnya kesadaran pengguna terhadap keamanan informasi, yang justru sering menjadi faktor utama terjadinya insiden kebocoran data pasien [8], [14]. Berdasarkan keterbatasan kajian terdahulu tersebut, penelitian ini memilih pendekatan deskriptif kualitatif untuk memperoleh pemahaman yang lebih mendalam mengenai penerapan keamanan data pasien pada SIMRS. Pendekatan kualitatif memungkinkan peneliti untuk mengeksplorasi secara langsung praktik keamanan sistem, kebijakan keamanan informasi, serta perilaku dan pemahaman pengguna SIMRS dalam konteks operasional rumah sakit sehari-hari [1], [13]. Dengan menganalisis data yang dihasilkan dari SIMRS, hasil observasi sistem, wawancara dengan tim teknologi informasi, serta studi dokumentasi kebijakan keamanan, penelitian ini diharapkan mampu mengidentifikasi kerentanan keamanan yang tidak selalu terungkap melalui pendekatan teknis semata. Oleh karena itu, penelitian ini dilakukan untuk mengevaluasi pengelolaan keamanan data pasien pada SIMRS, mengidentifikasi kerentanan baik dari aspek teknis maupun non-teknis, serta merumuskan strategi mitigasi yang relevan guna mencegah kebocoran data pasien dan meningkatkan keamanan informasi rumah sakit secara berkelanjutan di tengah meningkatnya ancaman serangan siber [6], [9].

2. METODE PENELITIAN

2.1. Desain Penelitian

Penelitian ini menggunakan metode studi kasus dengan pendekatan deskriptif kualitatif. Pendekatan ini dipilih untuk memperoleh gambaran menyeluruh mengenai penerapan keamanan data pasien pada SIMRS, termasuk aspek teknis, kebijakan, dan sumber daya manusia.

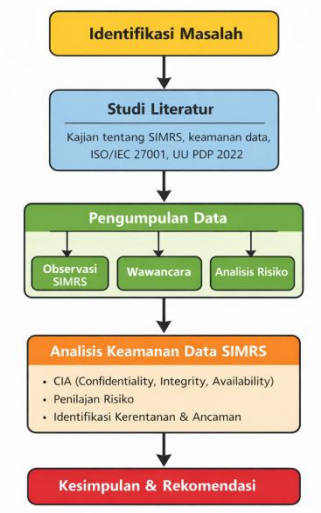
2.2. Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui:

1. Observasi sistem, untuk mengidentifikasi mekanisme keamanan pada SIMRS.
2. Wawancara mendalam, dengan tim TI dan manajemen rumah sakit terkait kebijakan keamanan data.
3. Studi dokumentasi, terhadap SOP, kebijakan keamanan informasi, dan regulasi yang berlaku.

2.3. Teknik Analisis Data

Analisis data dilakukan secara deskriptif dengan membandingkan kondisi eksisting keamanan SIMRS dengan prinsip keamanan informasi (Confidentiality, Integrity, Availability) serta standar keamanan informasi.



Gambar 1.Tahapan Penelitan Analisis Keamanan dta Pasien

Gambar 1 menunjukkan alur penelitian Analisis Keamanan Data Pasien pada Sistem Informasi Manajemen Rumah Sakit (SIMRS) yang disusun secara sistematis untuk memastikan proses penelitian berjalan terstruktur dan sesuai dengan tujuan penelitian. Flowchart ini menggambarkan tahapan penelitian mulai dari tahap awal hingga tahap akhir, yang saling berkaitan satu sama lain.

Tahap pertama adalah identifikasi masalah, di mana peneliti mengidentifikasi permasalahan utama terkait keamanan data pasien pada SIMRS, seperti potensi kebocoran data, kelemahan kontrol akses, serta risiko

serangan siber. Tahap ini dilakukan melalui pengamatan awal terhadap sistem dan proses pengelolaan data pasien di rumah sakit.

Tahap selanjutnya adalah studi literatur, yang bertujuan untuk memperoleh landasan teoritis dan konseptual terkait keamanan data pasien, SIMRS, serta standar dan regulasi yang berlaku. Studi literatur mencakup kajian terhadap jurnal ilmiah, standar keamanan informasi seperti ISO/IEC 27001, serta regulasi nasional seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Hasil studi literatur digunakan sebagai acuan dalam penyusunan instrumen penelitian dan analisis data.

Setelah studi literatur, penelitian dilanjutkan dengan pengumpulan data. Pada tahap ini, data dikumpulkan melalui tiga teknik utama, yaitu observasi terhadap sistem SIMRS, wawancara dengan tim teknologi informasi dan manajemen rumah sakit, serta studi dokumentasi terhadap kebijakan dan Standar Operasional Prosedur (SOP) keamanan data. Tahap ini bertujuan untuk memperoleh data empiris mengenai kondisi nyata penerapan keamanan data pasien.Tahap berikutnya adalah analisis data keamanan SIMRS. Data yang telah dikumpulkan dianalisis menggunakan pendekatan deskriptif dengan mengacu pada prinsip keamanan informasi, yaitu confidentiality, integrity, dan availability (CIA). Pada tahap ini dilakukan identifikasi risiko keamanan, evaluasi kontrol keamanan yang telah diterapkan, serta penilaian kesesuaian sistem dengan standar keamanan informasi.Berdasarkan hasil analisis, penelitian memasuki tahap perumusan solusi dan strategi mitigasi. Pada tahap ini, peneliti merumuskan rekomendasi teknis dan manajerial untuk meningkatkan keamanan data pasien pada SIMRS, seperti penerapan kontrol akses berbasis peran, enkripsi data, monitoring sistem secara real-time, serta peningkatan kompetensi sumber daya manusia. Tahap terakhir dalam flowchart adalah penyusunan kesimpulan dan rekomendasi. Pada tahap ini, peneliti menyusun kesimpulan berdasarkan hasil analisis dan pembahasan, serta memberikan rekomendasi yang dapat diterapkan oleh rumah sakit sebagai upaya perbaikan dan peningkatan keamanan data pasien secara berkelanjutan.

3. HASIL DAN ANALISIS

3.1. Penerapan Keamanan Data Pasien pada SIMRS

Hasil penelitian menunjukkan bahwa rumah sakit telah menerapkan mekanisme login pengguna dan pembatasan hak akses. Namun, pengelolaan kata sandi dan audit akses masih belum dilakukan secara optimal.

3.2 Risiko dan Ancaman Keamanan Data

Risiko utama yang ditemukan meliputi penggunaan akun bersama, kurangnya enkripsi data, serta minimnya monitoring aktivitas sistem. Kondisi ini berpotensi menimbulkan kebocoran data pasien.

3.3 Strategi Peningkatan Keamanan Data Pasien

Berdasarkan hasil analisis, strategi peningkatan keamanan data pasien pada SIMRS meliputi aspek teknis, manajerial, dan sumber daya manusia.

a. Penguatan Kontrol Akses
   Penerapan manajemen akses berbasis peran (*role-based access control*) untuk membatasi hak akses pengguna sesuai tugas dan tanggung jawab.
b. Enkripsi dan Perlindungan Data
   Penerapan enkripsi data pada penyimpanan dan transmisi data pasien untuk mencegah kebocoran informasi.
c. Monitoring dan Audit Sistem
   Monitoring aktivitas sistem secara real-time serta audit keamanan berkala untuk mendeteksi potensi ancaman
d. Penyusunan SOP dan Kebijakan Keamanan
   Penyusunan SOP keamanan data pasien dan kebijakan penanganan insiden keamanan informasi.
e. Peningkatan Kompetensi SDM
   Pelatihan rutin bagi staf TI dan pengguna SIMRS terkait keamanan informasi dan perlindungan data pasien.

Tabel 1. Risiko dan Mitigasi Keamanan Data SIMRS

Risiko Keamanan	Risiko Keamanan	Risiko Keamanan
Akses tidak sah	Kebocoran data pasien	Kontrol akses berbasis peran
Serangan malware	Gangguan layanan	Antivirus dan firewall
Kesalahan pengguna	Kehilangan data	Pelatihan dan SOP
Kegagalan sistem	Downtime SIMRS	Backup dan DRP

Tabel 2. Indikator Keamanan Data Pasien pada SIMRS

Aspek Keamanan	Kode	Indikator
Confidentiality	C1	Autentikasi pengguna (login)
Confidentiality	C2	Pengelolaan username dan password
Confidentiality	C3	Kontrol akses berbasis peran
Integrity	I1	Validasi perubahan data
Integrity	I2	Pencatatan log aktivitas pengguna
Availability	A1	Ketersediaan sistem SIMRS
Availability	A2	Backup data pasien
Availability	A3	Rencana pemulihan bencana (DRP)

Tabel 2 menyajikan indikator yang digunakan untuk menilai tingkat keamanan data pasien pada Sistem Informasi Manajemen Rumah Sakit (SIMRS). Indikator-indikator tersebut disusun berdasarkan prinsip keamanan informasi *confidentiality, integrity, dan availability* (CIA). Pada aspek confidentiality, indikator difokuskan pada mekanisme autentikasi pengguna, pengelolaan kredensial, dan pembatasan hak akses berbasis peran untuk memastikan bahwa data pasien hanya dapat diakses oleh pihak yang berwenang. Aspek integrity menilai keandalan sistem dalam menjaga keutuhan data melalui validasi perubahan data dan pencatatan aktivitas pengguna. Sementara itu, aspek *availability* menilai kesiapan sistem dalam menjamin ketersediaan data melalui mekanisme backup dan rencana pemulihan bencana. Indikator pada tabel ini menjadi dasar dalam proses pengumpulan dan analisis data keamanan SIMRS.

Tabel 3. Skala Penilaian Keamanan Data SIMRS

Skor	Kategori
1	Sangat Tidak Aman
2	Tidak Aman
3	Cukup
4	Aman
5	Sangat Aman

Tabel 2 menjelaskan skala penilaian yang digunakan dalam mengevaluasi tingkat keamanan data pasien pada SIMRS. Skala ini menggunakan rentang nilai 1 hingga 5, di mana nilai yang lebih tinggi menunjukkan tingkat keamanan yang lebih baik. Penggunaan skala ini bertujuan untuk memberikan gambaran kuantitatif terhadap kondisi keamanan sistem secara deskriptif. Skala penilaian ini memudahkan peneliti dalam mengelompokkan hasil evaluasi ke dalam kategori sangat tidak aman hingga sangat aman, sehingga memudahkan proses interpretasi hasil dan perumusan rekomendasi perbaikan keamanan.

Tabel 3 Hasil Evaluasi Keamanan Data Pasien pada SIMRS

Unit Kerja	Modul SIMRS	*Confidentiality*	*Integrity*	*Availability*
Pendaftaran	Pendaftaran Pasien	3	3	4
Rawat Inap	Rekam Medis	3	3	3
Farmasi	Farmasi	4	4	4
Poliklinik	Rekam Medis	4	4	3
Unit TI	Seluruh Modul	5	5	5

Tabel 3 menunjukkan hasil evaluasi tingkat keamanan data pasien pada SIMRS berdasarkan unit kerja dan modul sistem yang digunakan. Hasil penilaian memperlihatkan adanya variasi tingkat keamanan antar unit kerja. Unit pendaftaran dan rawat inap menunjukkan nilai keamanan yang masih berada pada kategori cukup, khususnya pada aspek *confidentiality* dan *integrity*. Hal ini mengindikasikan adanya kelemahan pada pengelolaan hak akses dan pencatatan aktivitas pengguna. Sebaliknya, unit teknologi informasi (TI) memperoleh nilai tertinggi pada seluruh aspek keamanan karena memiliki kontrol teknis dan pemahaman keamanan yang lebih baik. Temuan ini menunjukkan bahwa tingkat keamanan SIMRS sangat dipengaruhi oleh peran pengguna dan tingkat penguasaan sistem.

Tabel 4. Risiko dan Mitigasi Keamanan Data SIMRS

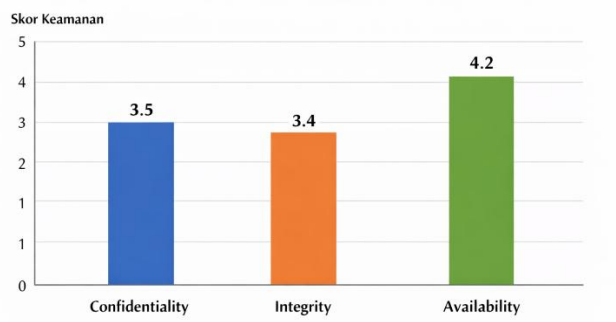
Risiko Keamanan	Dampak	Strategi Mitigasi
Akses tidak sah	Kebocoran data pasien	Kontrol akses berbasis peran
Serangan malware	Gangguan layanan SIMRS	Antivirus dan firewall
Kesalahan pengguna	Kehilangan data	Pelatihan dan SOP
Kegagalan system	*Downtime* SIMRS	Backup data dan DRP

Tabel 4 menggambarkan jenis risiko keamanan data pasien yang berpotensi terjadi pada SIMRS beserta dampak dan strategi mitigasinya. Risiko akses tidak sah menjadi ancaman utama yang dapat menyebabkan kebocoran data pasien, sehingga diperlukan penerapan kontrol akses berbasis peran. Risiko lain seperti serangan malware dan kesalahan pengguna dapat mengganggu layanan SIMRS dan menyebabkan kehilangan data, sehingga dibutuhkan perlindungan sistem berupa antivirus, firewall, serta pelatihan dan penerapan SOP yang jelas. Selain itu, kegagalan sistem yang menyebabkan *downtime* dapat diminimalkan melalui penerapan mekanisme backup data dan *disaster recovery plan*. Tabel ini menegaskan pentingnya pendekatan keamanan yang terintegrasi antara aspek teknis dan manajerial.

Tabel 5. Kesesuaian Keamanan SIMRS terhadap Prinsip CIA

Prinsip	Kondisi Eksisting	Keterangan
Confidentiality	Cukup	Kontrol akses belum optimal
Integrity	Cukup	*Audit log* belum menyeluruh
Availability	Baik	Sistem jarang mengalami downtime

Tabel 5 menyajikan tingkat kesesuaian penerapan keamanan SIMRS terhadap prinsip *confidentiality, integrity, dan availability.* Hasil evaluasi menunjukkan bahwa aspek availability berada pada kategori baik karena sistem relatif stabil dan jarang mengalami gangguan layanan. Namun, aspek *confidentiality* dan *integrity* masih berada pada kategori cukup, yang menandakan perlunya peningkatan pada kontrol akses, enkripsi data, dan audit log sistem. Temuan ini menunjukkan bahwa meskipun SIMRS telah mendukung operasional rumah sakit, penerapan keamanan informasi masih memerlukan penguatan agar sesuai dengan standar dan regulasi yang berlaku.



Gambar 2. Hasil Evaluasi Keamanan Data Pasien pada SIMRS Berdsasakan prinsip CIA

Gambar 2 menunjukkan hasil evaluasi tingkat keamanan data pasien pada Sistem Informasi Manajemen Rumah Sakit (SIMRS) berdasarkan prinsip *Confidentiality*, *Integrity*, dan *Availability* (CIA). Hasil penilaian memperlihatkan bahwa aspek availability memperoleh skor tertinggi sebesar 4,2, yang menunjukkan bahwa ketersediaan sistem dan akses layanan SIMRS telah berjalan dengan baik dan relatif stabil. Sementara itu, aspek *confidentiality* dan *integrity* masing-masing memperoleh skor 3,5 dan 3,4, yang berada pada kategori cukup. Hal ini mengindikasikan bahwa perlindungan terhadap kerahasiaan data pasien serta mekanisme penjagaan keutuhan data masih memerlukan peningkatan, khususnya dalam penerapan kontrol akses berbasis peran, enkripsi data, serta pencatatan dan audit aktivitas pengguna. Secara keseluruhan, grafik ini menunjukkan bahwa meskipun SIMRS telah mendukung operasional rumah sakit dengan baik dari sisi ketersediaan sistem, penguatan keamanan data pasien secara menyeluruh masih diperlukan agar sistem memenuhi standar keamanan informasi dan regulasi perlindungan data yang berlaku.

4. KESIMPULAN

4.1 Kesimpulan

Berdasarkan hasil analisis keamanan data pasien pada Sistem Informasi Manajemen Rumah Sakit (SIMRS), dapat disimpulkan bahwa penerapan SIMRS telah memberikan dukungan yang signifikan terhadap pengelolaan layanan dan integrasi data di rumah sakit. Namun demikian, aspek keamanan data pasien masih memerlukan perhatian dan peningkatan yang berkelanjutan. Evaluasi yang dilakukan berdasarkan prinsip keamanan informasi *confidentiality, integrity, dan availability* (CIA) menunjukkan bahwa tingkat keamanan SIMRS berada pada kategori cukup hingga baik, dengan variasi penerapan pada setiap unit kerja. Hasil penelitian menunjukkan bahwa aspek availability telah diterapkan dengan relatif baik, ditunjukkan oleh

stabilitas sistem dan minimnya gangguan layanan. Sebaliknya, aspek *confidentiality* dan *integrity* masih menghadapi beberapa kelemahan, terutama pada pengelolaan hak akses pengguna, penggunaan akun bersama, belum optimalnya penerapan enkripsi data, serta keterbatasan mekanisme audit dan pencatatan aktivitas sistem. Kondisi ini berpotensi menimbulkan risiko akses tidak sah, kebocoran data pasien, dan penurunan kepercayaan terhadap sistem informasi rumah sakit. Analisis risiko juga menunjukkan bahwa ancaman utama keamanan SIMRS berasal dari faktor teknis dan non-teknis, termasuk akses tidak sah, serangan malware, kesalahan pengguna, dan potensi kegagalan sistem. Temuan ini menegaskan bahwa keamanan data pasien tidak hanya bergantung pada teknologi yang digunakan, tetapi juga pada kebijakan organisasi dan kompetensi sumber daya manusia yang mengoperasikan sistem. Dengan demikian, penelitian ini menyimpulkan bahwa peningkatan keamanan data pasien pada SIMRS harus dilakukan secara komprehensif dan terintegrasi, mencakup penguatan kebijakan dan tata kelola keamanan informasi, peningkatan infrastruktur teknologi pendukung, serta pengembangan kesadaran dan kompetensi sumber daya manusia. Penerapan langkah-langkah tersebut diharapkan mampu meminimalkan risiko keamanan data, menjaga kerahasiaan dan keutuhan informasi pasien, serta menjamin ketersediaan sistem secara berkelanjutan sesuai dengan regulasi dan standar keamanan informasi yang berlaku.

4.2 Rekomendasi

Berdasarkan hasil analisis keamanan data pasien pada Sistem Informasi Manajemen Rumah Sakit (SIMRS), terdapat beberapa rekomendasi strategis yang dapat diterapkan oleh rumah sakit guna meningkatkan perlindungan data pasien secara menyeluruh dan berkelanjutan.

Pertama,rumah sakit disarankan untuk memperkuat kebijakan dan tata kelola keamanan informasi dengan menyusun serta menerapkan kebijakan keamanan data pasien yang terdokumentasi secara formal. Kebijakan tersebut harus mencakup pengelolaan hak akses pengguna, klasifikasi data pasien, prosedur penanganan insiden keamanan informasi, serta mekanisme evaluasi dan penegakan kepatuhan terhadap kebijakan yang telah ditetapkan.

Kedua, dari sisi teknis, rumah sakit perlu meningkatkan infrastruktur teknologi informasi dengan menerapkan kontrol akses berbasis peran *(role-based access control),* penggunaan autentikasi yang lebih kuat, serta penerapan enkripsi data pasien baik pada saat penyimpanan maupun transmisi data. Selain itu, penggunaan sistem keamanan jaringan seperti firewall, antivirus, dan sistem deteksi intrusi perlu dioptimalkan untuk mencegah ancaman serangan siber.

Ketiga, rumah sakit disarankan untuk melakukan monitoring dan audit keamanan sistem secara berkala. Penerapan mekanisme pencatatan dan pemantauan aktivitas pengguna (*logging* dan audit *trail*) secara real-time penting untuk mendeteksi potensi akses tidak sah serta sebagai dasar evaluasi keamanan SIMRS. Audit keamanan secara berkala juga diperlukan untuk menilai kesesuaian sistem dengan standar keamanan informasi yang berlaku.

Keempat, peningkatan kompetensi dan kesadaran sumber daya manusia menjadi faktor penting dalam menjaga keamanan data pasien. Rumah sakit perlu menyelenggarakan pelatihan dan sosialisasi secara rutin bagi seluruh pengguna SIMRS terkait keamanan informasi, perlindungan data pasien, dan prosedur penggunaan sistem yang aman guna meminimalkan risiko kesalahan manusia *(human error).*

Kelima, untuk menjamin ketersediaan dan keberlanjutan layanan, rumah sakit perlu menyusun dan mengimplementasikan mekanisme pencadangan data (backup) serta rencana pemulihan bencana (Disaster *Recovery Plan*) secara terstruktur dan terdokumentasi. Langkah ini bertujuan untuk memastikan data pasien tetap aman dan dapat diakses kembali apabila terjadi gangguan sistem, serangan siber, atau kondisi darurat lainnya.

Secara keseluruhan, penerapan rekomendasi ini diharapkan dapat membantu rumah sakit dalam membangun sistem keamanan data pasien yang kuat, terintegrasi, dan sesuai dengan regulasi serta standar keamanan informasi, sehingga SIMRS dapat berfungsi secara optimal dalam mendukung pelayanan kesehatan yang aman dan berkualitas.

DAFTAR PUSTAKA

[1] Anita Sriwaty Pardede, “Analisis Penerapan Sistem Informasi Manajemen Rumah Sakit (SIMRS) terhadap Kinerja Pelayanan Kesehatan di Rumah Sakit X,” *Detector: Jurnal Inovasi Riset Ilmu Kesehatan*, vol. 3, no. 3, pp. 157–168, Aug. 2025, doi: 10.55606/detector.v3i3.5573.

[2] S. Llorente and J. Delgado, “Implementation of Privacy and Security for a Genomic Information System Based on Standards,” *J Pers Med*, vol. 12, no. 6, Jun. 2022, doi: 10.3390/jpm12060915.

[3] S. Llorente and J. Delgado, “Implementation of Privacy and Security for a Genomic Information System Based on Standards,” *J Pers Med*, vol. 12, no. 6, Jun. 2022, doi: 10.3390/jpm12060915.

[4] R. Amalia, S. Lestari, and A. P. Tinggi, “Optimizing the Success of Hospital Management Information Systems in the Digitalization Era,” 2024.

[5] R. P. Amzar and N. Legowo, "Risk-Based Evaluation of Hospital Management Information System Implementation Using ISO 31000 Framework," *Jurnal Ilmiah Manajemen Kesatuan*, vol. 13, no. 6, pp. 5179–5190, Nov. 2025, doi: 10.37641/jimkes.v13i6.4221.

[6] D. Persetujuan Bersama, "FRESIDEN REPUBLIK INDONESIA 2-DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA dan PRESIDEN REPUBLIK INDONESIA."

[7] M. Javeedullah, "Emerging Technologies in AI and Machine Learning Security and Privacy in Health Informatics: Safeguarding Patient Data in a Digital World," *AlgoVista: Journal of AI & Computer Science*, vol. 2, no. 3, p. 2025.

[8] E. Z. Snigdha *et al.*, "Cybersecurity in Healthcare IT Systems: Business Risk Management and Data Privacy Strategies," *The American Journal of Engineering and Technology*, vol. 07, no. 03, pp. 163–184, Mar. 2025, doi: 10.37547/tajet/Volume07Issue03-15.

[9] R. Nur Akmal, D. Dwi Susilo, and E. Halma Rouf, "Evaluasi Keamanan Sistem Informasi Rumah Sakit: Metode Pengujian ISO 27001 di RS Khusus Mata Purwokerto," 2025. [Online]. Available: https://journal.stmiki.ac.id

[10] Dr. M. L. Schafer and Dr. J. Schafer, "Combining Frameworks to Improve Military Health System Quality and Cybersecurity," *Military Cyber Affairs*, vol. 6, no. 1, May 2023, doi: 10.5038/2378-0789.6.1.1088.

[11] "Future-Proofing Healthcare: The Role of AI and Blockchain in Data Security," 2025, doi: 10.15680/IJMRSET.2025.0803010.

[12] M. A. Algiffary, M. I. Herdiansyah, and Y. N. Kunang, "Hospital Management Information System Security Audit with COBIT 2019 Framework at RSUD Palembang Bari," *Journal of Applied Computer Science and Technology (Jacost)*, vol. 4, no. 1, pp. 19–26, 2023.

[13] C. Hidayatuloh, Sedarmayanti, and W. Utoyo, "Analisis Sistem Informasi Manajemen Rumah Sakit (SIMRS) Terhadap Peningkatan Layanan Kesehatan Dalam Mendukung Implementasi Rekam Medis Elektronik Di Era Digital," *INNOVATIVE: Journal Of Social Science Research*, vol. 5, pp. 11285–11303, 2025.

[14] D. Idryareza Augustyana and K. Mulyani, "Evaluasi Implementasi SIMRS dan Hambatannya di Instalasi Rawat Jalan RS Bhayangkara Balikpapan," *JMIAK: Jurnal Manajemen Informasi dan Administrasi Kesehatan*, vol. 8, no. 1, pp. 77–84, 2025.