Jurnal Rekam Medis dan Informasi Kesehatan
e-ISSN: 3110-228X

Identifikasi Risiko Keamanan Data Akibat Penggunaan Password Yang Tidak Kuat Pada Pengguna SIMRS: *Systematic Literature Review*

Identifying Data Security Risks from Using Weak Passwords by SIMRS Users: Systematic Literature Review

Rheina Arfiandita1 ,Wahyu Wijaya Widiyanto2

1 Politeknik Indonusa Surakarta
2Politeknik Indonusa Surakarta
Korespondensi e-mail:f22071@poltekindonusa.ac.id

ABSTRAK

Perkembangan Sistem Informasi Manajemen Rumah Sakit (SIMRS) memberikan manfaat besar dalam pengelolaan data rekam medis elektronik, namun di sisi lain meningkatkan risiko keamanan data, khususnya akibat penggunaan password yang tidak kuat. Penelitian ini bertujuan untuk mengidentifikasi risiko keamanan data yang ditimbulkan oleh lemahnya pengelolaan password pada pengguna SIMRS. Metode yang digunakan adalah *Systematic Literature Review* (SLR) dengan pendekatan PRISMA, melalui penelusuran artikel ilmiah pada basis data Google Scholar periode 2021–2025. Proses seleksi menghasilkan lima artikel yang memenuhi kriteria inklusi untuk dianalisis secara kualitatif. Hasil kajian menunjukkan bahwa penggunaan password lemah, tidak diganti secara berkala, serta pengelolaan autentikasi yang kurang optimal berkontribusi signifikan terhadap risiko kebocoran data, akses tidak sah, dan serangan siber seperti brute force, phishing, dan social engineering. Selain faktor teknis, faktor manusia dan kebijakan keamanan yang belum ketat turut memperbesar risiko keamanan SIMRS. Kesimpulan penelitian ini menegaskan bahwa penguatan kebijakan password, penerapan teknologi keamanan tambahan, serta peningkatan kesadaran pengguna sangat diperlukan untuk melindungi data rekam medis secara optimal.

Kata kunci: keamanan data, password lemah, SIMRS, rekam medis elektronik, keamanan siber

ABSTRACT

The development of Hospital Management Information Systems (HMIS) has significantly improved the management of electronic medical records; however, it also increases data security risks, particularly due to weak password usage. This study aims to identify data security risks caused by inadequate password management among HMIS users. The research employed a Systematic Literature Review (SLR) method using the PRISMA approach by reviewing scientific articles published between 2021 and 2025 from the Google Scholar database. The selection process resulted in five eligible articles that were analyzed qualitatively. The findings indicate that weak passwords, infrequent password changes, and poor authentication management significantly contribute to data breaches, unauthorized access, and cyberattacks such as brute force, phishing, and social engineering. In addition to technical issues, human factors and insufficient security policies further increase vulnerabilities within HMIS. This study concludes that strengthening password policies, implementing additional security technologies, and improving user awareness are essential steps to ensure optimal protection of electronic medical record data.

Keywords: data security, weak passwords, hospital information systems, electronic medical records, cybersecurity

Pendahuluan

Perkembangan teknologi informasi (TI) yang pesat pada era globalisasi telah memengaruhi berbagai aspek kehidupan, termasuk bidang Kesehatan (Putra, 2023). Pemanfaatan TI dalam pelayanan kesehatan bertujuan untuk meningkatkan kecepatan, efisiensi, efektivitas, serta mutu layanan (Wawan Wardiana, 2002). Teknologi informasi membantu penyimpanan, pengolahan, dan penyebaran data secara digital sehingga memudahkan tenaga kesehatan dalam memberikan pelayanan yang lebih cepat dan akurat. Oleh karena itu, tenaga kesehatan perlu mampu mengikuti dan menerapkan perkembangan teknologi agar pelayanan semakin optimal. Penelitian ini bertujuan untuk mengkaji penerapan teknologi informasi dalam dunia Kesehatan (Siswati & Dindasari, 2019).

Keamanan sistem informasi rekam medis dicantumkan dalam Permenkes No. 24 Tahun 2022, terdapat 3 pasal yang menjelaskan keamanan rekam medis elektronik ialah dari pasal 29 hingga pasal 31. Pasal 29 Menegaskan bahwa penyelenggaraan RME harus menjaga kerahasiaan, integritas, dan ketersediaan data. Pasal 30, Mengatur hak akses tenaga kesehatan untuk menginput, memperbaiki, dan melihat data RME sesuai kebutuhan pelayanan. Pasal 31, Memperbolehkan penggunaan tanda tangan elektronik sebagai bentuk verifikasi dan keamanan data RME (Gemawaty & Yuliani, 2024).

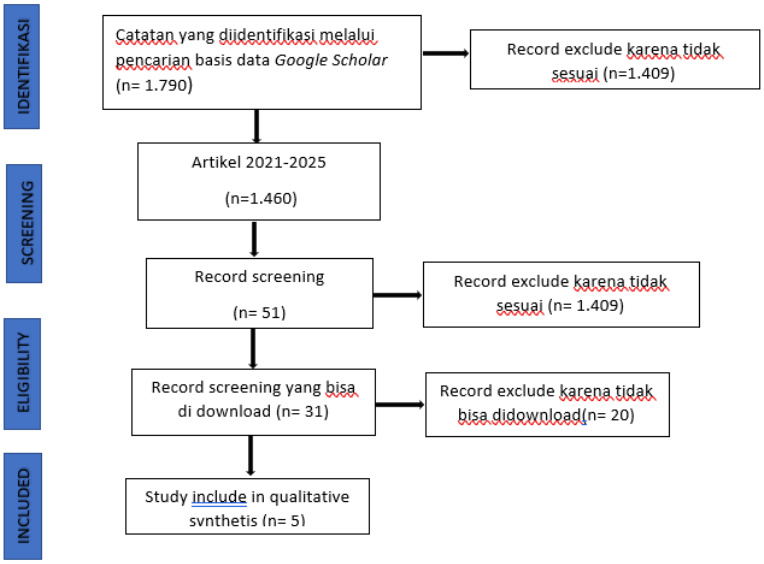
Keamanan data rekam medis memiliki peran yang sangat penting sehingga diperlukan berbagai langkah untuk memastikan informasi yang bersifat rahasia tidak dapat diakses oleh pihak yang tidak berwenang. Pelanggaran keamanan dapat menimbulkan dampak serius, khususnya bagi pasien, karena akses ilegal berpotensi menyebabkan kerugian besar (Baihaqy et al., 2025). Selain itu, risiko peretasan dapat memicu kerusakan atau hilangnya data, sedangkan perubahan isi rekam medis dapat menimbulkan kesalahpahaman baik dari pihak pasien maupun tenaga medis. Oleh karena itu, perlindungan rekam medis harus dilakukan secara optimal mengingat sifatnya yang sangat rahasia dan perlu dijaga dengan ketat (Wardani et al., 2024).

Keamanan data juga berkaitan dengan penggunaan username dan password yang seringkali rentan jika tidak dikelola dengan baik, kontrol akses yang kurang ketat terutama terkait perubahan atau penghapusan data oleh administrator, penerapan tanda tangan elektronik dan PIN *(Personal Identification Number)* (Baihaqy et al., 2025) yang belum maksimal, serta strategi backup data yang belum memadai dalam menghadapi risiko peretasan. Selain itu, pembatasan hak akses melalui user ID unik yang tidak selalu diterapkan secara efektif dan pencatatan aktivitas pengguna dalam log file yang kurang optimal menambah risiko kebocoran data (Baihaqy et al., 2025).

Berdasarkan permasalahan tersebut, penelitian ini dilakukan untuk mengidentifikasi risiko keamanan data akibat penggunaan password yang tidak kuat pada pengguna SIMRS di Rumah Sakit X. Penelitian juga merangkum temuan literatur tahun 2021–2025 mengenai praktik keamanan password, kebijakan autentikasi, serta celah keamanan yang umum terjadi pada sistem informasi kesehatan. Meskipun beberapa fasilitas kesehatan telah mengimplementasikan langkah-langkah ini, standar keamanan sering kali belum terpenuhi sepenuhnya. Oleh karena itu perlu dlakukannya pengembangan teknik baru dalam penggunaan password atau peningkatan dalam penerapan sistem keamanan untuk melindungi data pasien secara optimal.

Metode

Penelitian ini menggunakan metode studi literatur dengan pendekatan PRISMA *(Preferred Reporting Items for Systematic Reviews and Meta-Analysis)* (Simamora et al., 2024) untuk mengidentifikasi, menyeleksi, dan menganalisis artikel ilmiah yang relevan dengan topik. Pencarian literatur dilakukan melalui basis data Google Scholar. Kata kunci yang digunakan dalam proses pencarian meliputi: “kata sandi lemah”, “keamanan data rumah sakit”, “rekam medis elektronik”, “perlindungan sistem informasi”, dan “keamanan siber dalam layanan kesehatan”.



Gambar 1. Alur penelusuran artikel dengan pendekatan PRISMA

Hasil

Pada tahap identifikasi awal, diperoleh sebanyak 1.790 artikel dari hasil pencarian Google Scholar. Selanjutnya, dilakukan pembatasan tahun publikasi, yaitu artikel yang diterbitkan pada rentang 2021–2025, sehingga jumlah artikel yang tersisa menjadi 1.460 artikel. Dari 1.460 artikel tersebut, dilakukan screening berdasarkan judul dan abstrak untuk menilai kesesuaian dengan topik penelitian. Hasilnya, sebanyak 1.409 artikel dikeluarkan karena tidak relevan dengan fokus penelitian, sehingga tersisa 51 artikel yang masuk ke tahap screening lanjutan. Pada tahap ini, dilakukan penilaian terhadap ketersediaan teks lengkap (full text). Dari 51 artikel yang diseleksi, sebanyak 31 artikel dapat diunduh dan dianalisis lebih lanjut, sedangkan 20 artikel dikeluarkan karena tidak dapat diakses secara penuh. Setelah dilakukan penilaian kelayakan secara mendalam berdasarkan kesesuaian isi dengan tujuan penelitian, diperoleh 5 artikel yang memenuhi seluruh kriteria inklusi. Artikel-artikel tersebut kemudian dimasukkan dalam sintesis kualitatif untuk dianalisis dan dibahas lebih lanjut terkait isu keamanan siber dan perlindungan data pada sistem rekam medis elektronik di rumah sakit. Berikut untuk tabel artikel yang di review:

Tabel 1 Artikel Yang di *Review*

No	Penulis,Tahun	Judul	Metode Penelitian	Hasil Penelitian
1.	(Rochman et al., 2021)	Analisis Keamanan Website Dengan Information System Security Assessment Framework (Issaf) Dan Open Web Application Security Project (Owasp) Di	Metode ISSAF dan OWASP, tools Nikto, OWASP ZAP	Ditemukan celah keamanan utama berupa Cross-Site Scripting (XSS) dan information leakage. Pada uji autentikasi, sistem masih menampilkan error detail yang membuka informasi database. Ditemukan username dan password database pada fase exploit. Namun beberapa aspek aman: authorization testing, session management bekerja baik. Rekomendasi: pengujian berkala, filter port, peningkatan keamanan server, maintenance hardware/software, dan penggunaan antivirus original.

		Rumah Sakit Xyz		
2.	(Nur et al., 2025)	Implementasi Pengamanan Data Menggunakan Teknik Bcrypt Hashing Password dan Algoritma Advanced Encryption Standard (AES)	Metode Bcrypt Hashing, Algoritma AES-256	Password plaintext berubah menjadi 29 karakter hash dengan Bcrypt. AES menghasilkan ciphertext panjang sehingga lebih sulit ditembus. *Unit testing* menunjukkan: Hash tidak dapat dikembalikan ke bentuk asli dan Setiap hash selalu berbeda meskipun input sama. Sistem dinilai berhasil meningkatkan keamanan dan dapat mencegah serangan brute force & SQL injection..
3.	(We'e et al., 2023)	Evaluasi Aspek Keamanan Dan Kerahasiaan Rekam Medis Elektronik Di Rumah Sakit Panti Nugroho	Aspek keamanan informasi: 1. Confidentiality (kerahasiaan) 2. Integrity 3. Authentication 4. Availability 5. Access Control Non-repudiation	Confidentiality: telah berjalan baik melalui penggunaan user ID & password. Integrity: tersedia fitur edit data; kendala terjadi ketika sistem error. Authentication: hak akses diberikan sesuai unit kerja, namun masih perlu peningkatan pengelolaan ID. Availability: jika sistem error, petugas menggunakan rekam medis manual sementara. Access Control: hak akses berbeda tiap jabatan; sudah ada SOP. Non-repudiation: proses pelacakan perubahan data belum maksimal, meski log file tersedia di bagian IT. Sistem RME sudah berjalan baik tetapi masih membutuhkan optimalisasi fasilitas & infrastruktur, serta peningkatan pelatihan pengguna.
4.	(Rahma & Suryani, 2021)	Analisis Penggantian Password User Id Dalam Sistem Rekam Medis Elektronik Guna Menjaga Keamanan Data Rekam Medis Di Rumah Sakit Hermina Arcamanik	Keamanan data rekam medis elektronik (kerahasiaan, akses, integritas)	Penggantian password secara berkala efektif meningkatkan keamanan RME dan mencegah akses tidak sah. Masalah ditemukan karena staf sering lupa logout dan memakai User ID petugas lain, meningkatkan risiko penyalahgunaan akun. Dibutuhkan pelatihan keamanan, kebijakan ketat, dan sosialisasi perubahan password minimal 1 bulan sekali.
5.	(M.Yamin et al., 2023)	Evaluasi Risiko Pada Penggunaan Password Yang Lemah: Analisis Kasus Penggunaan	Risiko keamanan siber	Password lemah sangat rentan terhadap metode serangan siber seperti: social engineering, brute force, shoulder surfing, phishing, dan keylogger Solusi yang disarankan: Menggunakan password kompleks dan unik, Mengganti password

	Password Umum	secara berkala, Autentikasi dua fakto, Penggunaan password manager

Pembahasan

Berdasarkan hasil systematic literature review terhadap lima artikel terpilih, dapat diketahui bahwa keamanan data pada sistem informasi manajemen rumah sakit (SIMRS), khususnya sistem rekam medis elektronik (RME), masih menghadapi berbagai tantangan, terutama yang berkaitan dengan penggunaan password yang tidak kuat dan pengelolaan autentikasi pengguna. Temuan ini menunjukkan bahwa meskipun penerapan teknologi informasi di rumah sakit telah berkembang pesat, aspek keamanan sistem belum sepenuhnya diimplementasikan secara optimal .

Hasil penelitian (Rochman et al., 2021) menunjukkan bahwa celah keamanan pada sistem rumah sakit masih sering ditemukan, terutama pada sisi autentikasi dan pengelolaan informasi sensitif. Ditemukannya kerentanan berupa *Cross-Site Scripting (XSS)* dan kebocoran informasi database menandakan bahwa sistem autentikasi yang lemah, termasuk pengelolaan username dan password, dapat menjadi pintu masuk bagi serangan siber. Kondisi ini berpotensi mengancam kerahasiaan data rekam medis pasien, yang bersifat sangat sensitif dan dilindungi oleh regulasi kesehatan.

Selanjutnya, penelitian (Nur et al., 2025) menegaskan bahwa penguatan keamanan password melalui teknik enkripsi dan hashing seperti Bcrypt dan AES terbukti mampu meningkatkan keamanan sistem secara signifikan. Penggunaan hashing password yang tidak dapat dikembalikan ke bentuk asli serta enkripsi data yang kompleks mampu mencegah serangan brute force dan SQL injection. Temuan ini memperkuat bahwa password yang lemah dan disimpan tanpa perlindungan kriptografi yang memadai merupakan salah satu faktor utama penyebab kebocoran data pada sistem informasi kesehatan.

Penelitian (We'e et al., 2023) mengungkap bahwa aspek confidentiality dan access control pada RME telah diterapkan melalui penggunaan user ID dan password serta pembagian hak akses berdasarkan unit kerja. Namun, masih ditemukan kendala dalam aspek integrity dan non-repudiation, terutama ketika sistem mengalami gangguan teknis dan pencatatan log aktivitas pengguna belum dimanfaatkan secara optimal. Hal ini menunjukkan bahwa meskipun password telah digunakan sebagai mekanisme pengamanan dasar, tanpa pengelolaan sistem yang menyeluruh dan monitoring aktivitas pengguna, risiko penyalahgunaan akun tetap tinggi.

Sementara itu, penelitian (Rahma & Suryani, 2021) menyoroti pentingnya penggantian password secara berkala dalam menjaga keamanan data rekam medis elektronik. Temuan bahwa petugas sering menggunakan akun milik pengguna lain atau lupa melakukan logout menandakan bahwa faktor manusia (human error) masih menjadi penyebab dominan terjadinya pelanggaran keamanan sistem. Kondisi ini memperkuat bahwa keamanan password tidak hanya bergantung pada kompleksitas teknis, tetapi juga pada kedisiplinan dan kesadaran pengguna sistem.

Penelitian (M.Yamin et al., 2023) semakin menegaskan bahwa password yang lemah sangat rentan terhadap berbagai jenis serangan siber, seperti phishing, brute force, social engineering, dan keylogger. Rekomendasi penggunaan password kompleks, autentikasi dua faktor, serta password manager menjadi solusi yang relevan untuk diterapkan dalam sistem informasi rumah sakit. Hal ini sejalan dengan kebutuhan perlindungan sistem informasi kesehatan yang menuntut tingkat keamanan lebih tinggi dibandingkan sistem informasi pada umumnya.

Secara keseluruhan, hasil review menunjukkan bahwa penggunaan password yang tidak kuat merupakan salah satu faktor utama risiko keamanan data pada SIMRS dan RME. Selain aspek teknis, faktor kebijakan, pelatihan pengguna, serta pengawasan sistem juga berperan penting dalam menjaga keamanan data. Oleh karena itu, diperlukan pendekatan yang komprehensif, mencakup penguatan

teknologi keamanan, penerapan kebijakan yang ketat, serta peningkatan kesadaran dan kompetensi pengguna sistem, guna melindungi data rekam medis pasien secara optimal.

Simpulan

Berdasarkan hasil systematic literature review dengan pendekatan PRISMA, dapat disimpulkan bahwa penggunaan password yang lemah pada sistem informasi manajemen rumah sakit, khususnya rekam medis elektronik, masih menjadi risiko utama terhadap keamanan data pasien. Berbagai penelitian menunjukkan bahwa lemahnya pengelolaan password dapat membuka peluang terjadinya akses tidak sah, kebocoran data, serta serangan siber yang mengancam kerahasiaan, integritas, dan ketersediaan informasi kesehatan. Meskipun beberapa rumah sakit telah menerapkan mekanisme autentikasi dasar, penerapannya masih belum optimal dan memerlukan penguatan dari sisi teknis, kebijakan, serta perilaku pengguna.

Saran

Berdasarkan simpulan tersebut, disarankan agar pihak rumah sakit:

1. Menerapkan kebijakan penggunaan password yang kuat, meliputi kombinasi karakter, panjang minimal password, serta penggantian password secara berkala.
2. Mengimplementasikan teknologi keamanan tambahan, seperti hashing password, enkripsi data, dan autentikasi dua faktor untuk meningkatkan perlindungan sistem.
3. Meningkatkan pelatihan dan sosialisasi kepada pengguna SIMRS, khususnya terkait kesadaran keamanan informasi dan risiko penggunaan password yang lemah.
4. Mengoptimalkan pengelolaan hak akses dan pencatatan log aktivitas pengguna, sebagai upaya monitoring dan pencegahan penyalahgunaan akun.
5. Penelitian selanjutnya disarankan untuk mengkaji implementasi keamanan password secara langsung pada sistem SIMRS di rumah sakit, sehingga diperoleh gambaran yang lebih empiris dan aplikatif.

Daftar pustaka

Baihaqy, A. H. Al, Yuwana, M. A. S. A., Surya, A. P. A., & Fauzi, M. A. N. (2025). Analisa Dampak Kebocoran Data Pusat Data Nasional (Pdn) 2024 Dalam Perspektif Ham. *Wicarana*, *3*(1), 31–37. https://doi.org/10.57123/wicarana.v3i1.167

Gemawaty, C. A., & Yuliani, Y. (2024). Manajemen Identitas Dan Akses Dalam Keamanan Sistem Informasi (Pendekatan Literature Review). *Jurnal Manajemen Informatika Jayakarta*, *4*(4), 396–403. http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

M.Yamin, Malethi, T. T., Monica, Jodhika, & Natali, S. (2023). *Evaluasi Risiko Pada Penggunaan Password Yang Lemah: Analisis Kasus Penggunaan Password Umum*. *1*(1), 41–48.

Nur, K., Suhartono, D., Thoriq, M., & Qothrunnada, A. (2025). Implementasi Pengamanan Data Menggunakan Teknik Bcrypt Hashing Password dan Algoritma Advanced Encryption Standard (AES) Implementation of Data Security Using Bcrypt Hashing Password Technique and Advanced Encryption Standard (AES) Algorithm. *Jurnal Sistem Dan Teknologi Informasi*, *13*(1), 101–108. https://doi.org/10.26418/justin.v13i1.84997

Putra, R. S. (2023). *Kajian Penerapan Teknologi Informatika pada Dunia Kesehatan*. *3*(3), 180–187.

Rahma, A., & Suryani, A. I. (2021). *Analisis Penggantian Password User ID Dalam Sistem Rekam Medis Elektronik Guna Menjaga Keamanan Data Rekam Medis di Rumah Sakit Hermina Arcamanik*. *32*(3), 167–186.

Rochman, A., Salam, R. R., & Maulana, S. A. (2021). *Analisi Keamanan Website Dengan Information System Security Assesment Framework (ISSAF) dan Web Application Security Project (OWASP) di Rumah Sakit Xyz*. *2*(4), 6.

Simamora, S. C., Gaffar, V., & Arief, M. (2024). Systematic Literatur Review Dengan Metode Prisma: Dampak Teknologi Blockchain Terhadap Periklanan Digital. *JURNAL ILMIAH M-PROGRESS*, 1–11.

Siswati, & Dindasari, D. A. (2019). Tinjauan Aspek Keamanan dan Kerahasiaan Rekam Medis di Rumah Sakit Setia Mitra Jakarta Selatan Perekam Medis dan Informasi Kesehatan Bhumi Husada Jakarta. *Jurnal Rekam Medis Dan Informasi Kesehatan*, *2*(2), 91–99.

Wardani, E., Putra, D. H., Sonia, D., & Yulia, N. (2024). *Keamanan Sistem Informasi Rekam Medis*

Elektronik di Rumah Sakit Islam Jakarta Sukapura. *3*(2), 31–38.
Wawan Wardiana. (2002). Perkembangan Teknologi Informasi di Indonesia. *Academia.Edu*, 1–7. https://www.kompasiana.com/muhammad75161/63272f356e14f10616141444/perkembangan-teknologi-informasi-di-indonesia?lgn_method=google
We'e, A., Nugroho, R. H., & Siswatibudi, H. (2023). *Evaluasi Aspek Keamanan dan Kerahasiaan Rekam Medis Elektronik di Rumah Sakit Panti Nugroho*. *14*(November).