Jurnal Riset Sains dan Kesehatan Indonesia
E-ISSN: 3047-8855
DOI: https://doi.org/10.69930/jrski.v2i6.622
Research Article

ScienceTech. Group

Vol. 2 (6), 2025
Hal. 256-262

Analisis Penggantian Password RME untuk Keamanan Data di Unit Rawat Jalan RS Hermina Arcamanik

Moh Arya Putra Ramadhan *, Sali Setiatin

Program Studi Rekam Medis dan Informasi Kesehatan, Kesehatan, Politeknik Piksi Ganesha, Indonesia
*Email (Penulis Korespondensi): arya1putra2@gmail.com

Abstrak. *Rekam Medis Elektronik (RME) memegang peranan krusial dalam menunjang efisiensi pelayanan kesehatan modern, namun sistem ini juga menghadapi risiko tinggi terhadap ancaman keamanan data sensitif. Keamanan data pasien, terutama di Unit Rawat Jalan (URJ) yang menjadi gerbang utama interaksi dengan sistem, sangat bergantung pada mekanisme kontrol akses yang andal. Penelitian ini bertujuan untuk menganalisis implementasi dan mengevaluasi efektivitas kebijakan penggantian password User ID RME yang diterapkan dalam rangka menjaga kerahasiaan dan integritas data pasien di URJ RS Hermina Arcamanik. Metode penelitian ini menggunakan pendekatan deskriptif kualitatif. Pengumpulan data dilakukan melalui wawancara mendalam dengan petugas URJ, staf teknologi informasi (IT), serta observasi terhadap praktik dan standar operasional prosedur (SOP) terkait penggantian password. Analisis difokuskan pada tingkat kepatuhan pengguna terhadap kebijakan yang berlaku, identifikasi kendala teknis maupun non-teknis dalam implementasi, serta dampak nyata kebijakan tersebut terhadap upaya pencegahan akses data secara ilegal. Hasil penelitian ini diharapkan mampu memberikan gambaran komprehensif mengenai kondisi keamanan data RME terkait password di lingkungan studi. Lebih lanjut, temuan yang diperoleh akan digunakan untuk menyusun rekomendasi strategis guna optimalisasi kebijakan penggantian password RME. Tujuannya adalah memperkuat tata kelola keamanan informasi dan meningkatkan perlindungan data pasien di RS Hermina Arcamanik.*

Kata kunci: *RME; Keamanan Data; Password; Rawat Jalan*

Abstract. *The Electronic Medical Record (EMR) plays a crucial role in supporting the efficiency of modern health services, but this system also faces a high risk of sensitive data security threats. Patient data security, especially in the Outpatient Unit (OPD) which serves as the main gateway for system interaction, highly depends on reliable access control mechanisms. This research aims to analyze the implementation and evaluate the effectiveness of the EMR User ID password replacement policy enforced to maintain the confidentiality and integrity of patient data in the OPD of Hermina Arcamanik Hospital. The research method employs a qualitative descriptive approach. Data collection is carried out through in-depth interviews with OPD officers, information technology (IT) staff, and observation of practices and standard operating procedures (SOP) related to password replacement. The analysis focuses on the level of user compliance with the applicable policy, the identification of technical and non-technical constraints in the implementation, and the real impact of the policy on efforts to prevent illegal data access. The results of this study are expected to provide a comprehensive overview of the EMR data security condition related to password within the study environment. Furthermore, the findings will be utilized to formulate strategic recommendations for optimizing the EMR password replacement policy. The goal is to strengthen information security governance and enhance patient data protection at Hermina Arcamanik Hospital*

Received: 1 Desember 2025 / Accepted: 30 Desember 2025 / Available online: 31 Desember 2025

Keywords: *EMR; Data Security; Password; Outpatient Unit*

1. Pendahuluan

Rumah sakit merupakan sebuah institusi pelayanan kesehatan yang memberikan layanan kesehatan kepada individu secara menyeluruh. Layanan yang disediakan mencakup upaya promotif, preventif, kuratif, rehabilitatif, hingga paliatif (UU Nomor 17, 2023). Selain itu, rumah sakit juga menyediakan fasilitas untuk perawatan inap, perawatan jalan, serta penanganan kegawatdaruratan. Rumah sakit memiliki tujuan untuk meningkatkan kinerja dan efisiensi layanan kesehatan dengan memanfaatkan inovasi teknologi serta menerapkan sistem manajemen rumah sakit yang terintegrasi secara menyeluruh (Nugroho, 2025).

RS Hermina Arcamanik merupakan salah satu rumah sakit swasta di Indonesia yang telah mengimplementasikan sistem digital dalam pelayanan kesehatan, khususnya melalui penggunaan RME. Langkah ini mencerminkan komitmen rumah sakit dalam meningkatkan mutu pelayanan, efisiensi operasional, serta integrasi data pasien secara menyeluruh. Penggunaan RME sebagai komponen dalam sistem informasi kesehatan berbasis komputer di fasilitas pelayanan kesehatan memberikan berbagai keuntungan signifikan dalam upaya meningkatkan mutu layanan. RME memfasilitasi penyimpanan dan akses data medis pasien secara efisien, tepat, dan tersusun dengan baik (Camila dan Anggraini, 2025). Namun, seiring dengan semakin berkembangnya digitalisasi di sektor kesehatan, tantangan baru pun muncul, khususnya terkait perlindungan terhadap data dan informasi medis pasien yang bersifat sangat sensitif dan pribadi.

Rekam Medis Elektronik sebagai sistem berbasis teknologi informasi menyimpan berbagai data penting seperti identitas pasien, diagnosa, hasil pemeriksaan laboratorium, tindakan medis, hingga riwayat pengobatan. Oleh karena itu, Keamanan dalam pengelolaan sistem informasi merupakan hal yang sangat penting guna memastikan data kesehatan pasien tetap rahasia, utuh, dan selalu dapat diakses saat dibutuhkan(Wilar et al., 2023).

Salah satu komponen mendasar dalam sistem keamanan tersebut adalah manajemen autentikasi pengguna, terutama pengelolaan *password* pada *User ID* tenaga kesehatan yang memiliki akses terhadap RME. *Password* berfungsi sebagai garis pertahanan pertama untuk mencegah akses tidak sah ke dalam sistem. Namun, dalam praktiknya, masih banyak dijumpai penggunaan *password* yang lemah, penggunaan *password* yang sama secara berulang di berbagai sistem, serta minimnya frekuensi penggantian *password*. Kondisi ini dapat membuka peluang terjadinya kebocoran atau penyalahgunaan data oleh pihak yang tidak berwenang.

Oleh sebab itu, kebijakan penggantian *password* secara berkala menjadi salah satu langkah penting dalam memperkuat sistem pertahanan keamanan informasi. Penerapan kebijakan ini tidak hanya perlu dilihat dari sisi administratif sebagai bentuk kepatuhan terhadap prosedur, namun juga harus mencakup pertimbangan teknis seperti kompleksitas *password*, validitas durasi penggunaannya, hingga dukungan sistem yang memungkinkan otomatisasi pengingat penggantian. Selain itu, keberhasilan pelaksanaan kebijakan ini juga sangat bergantung pada kesadaran dan disiplin pengguna dalam menjaga keamanan akses mereka, yang dalam konteks rumah sakit melibatkan tenaga medis, petugas administrasi, dan pihak manajemen.

Dalam kerangka hukum di Indonesia, perlindungan terhadap data rekam medis pasien telah diatur dalam sejumlah regulasi nasional. Seperti yang dijelaskan Peraturan

Pemerintah Nomor 71 Tahun 2019 tentang penyelenggaraan sistem dan transaksi elektronik mewajibkan setiap penyelenggara sistem elektronik untuk menjamin keamanan sistem serta perlindungan data pribadi pengguna(PP RI NO 71, 2019). Dengan demikian, rumah sakit sebagai institusi yang mengelola data pasien dalam sistem elektronik memiliki tanggung jawab hukum, profesional, dan etis untuk melindungi informasi tersebut dari berbagai bentuk ancaman, baik internal maupun eksternal.

Dalam konteks tersebut, RS Hermina Arcamanik menjadi studi kasus yang relevan untuk meninjau bagaimana pelaksanaan kebijakan penggantian *password* pada sistem RME diterapkan. Penelitian ini bertujuan untuk menganalisis secara mendalam bagaimana mekanisme penggantian *password* di implementasikan, sejauh mana kebijakan tersebut dipatuhi oleh pengguna sistem, tantangan apa saja yang dihadapi dalam pelaksanaannya, serta apakah kebijakan tersebut telah sejalan dengan standar keamanan informasi dan regulasi yang berlaku di Indonesia. Hasil penelitian ini diharapkan dapat memberikan gambaran yang lebih jelas mengenai praktik keamanan data di rumah sakit, sekaligus menjadi dasar perumusan strategi yang lebih efektif dalam melindungi informasi pasien melalui penguatan sistem autentikasi pengguna.

2. Metode

Jenis metode penelitian yang di gunakan adalah metode kualitatif dengan pendekatan deskriptif. Metode kualitatif adalah pendekatan penelitian di mana peneliti secara langsung menyelidiki sumber data atau responden berdasarkan temuan lapangan (Rahma dan Suryani, 2024). Pendekatan deskriptif dimaksudkan untuk menjelaskan secara rinci fenomena yang berlangsung secara alami, agar peneliti mampu menangkap makna yang tersembunyi di balik perilaku, aktivitas, dan interaksi sosial yang diamati(Sugiyono, 2020). Data dikumpulkan dengan melakukan wawancara secara mendalam kepada responden, di mana proses wawancara direkam menggunakan alat perekam (Setiatin, Seli dan Kusuma, 2025). Wawancara merupakan metode untuk menggali informasi secara mendalam terkait pandangan atau pengalaman responden melalui interaksi tatap muka, namun efektivitasnya sangat dipengaruhi oleh kemampuan komunikasi peneliti dan memiliki risiko munculnya bias (Romdona et al., 2025). Wawancara bertujuan untuk memahami secara lebih mendalam pemikiran, pengalaman, dan sudut pandang partisipan penelitian. Metode ini memberi peneliti kesempatan untuk menangkap detail kontekstual dan makna yang mungkin terlewat jika hanya menggunakan metode lain (Mudasir, 2024).

3. Hasil dan Pembahasan

RME merupakan salah satu komponen yang sangat krusial dalam sistem pengelolaan informasi pasien di Rumah Sakit Umum (RSU) Hermina Arcamanik. RME memegang peranan penting dalam mendukung efisiensi serta efektivitas proses penyimpanan dan pengaksesan data medis(Rahma dan Mayesti, 2019).

Penggunaan sistem ini memungkinkan tenaga kesehatan untuk memperoleh informasi pasien dengan cepat dan akurat, yang pada gilirannya meningkatkan kualitas pelayanan medis. Meskipun RME menawarkan banyak keunggulan dari sisi efisiensi operasional, aspek keamanan data pasien menjadi hal yang tidak kalah penting. Salah satu langkah strategis yang dapat diterapkan dalam menjaga kerahasiaan serta integritas data pasien dalam sistem elektronik adalah dengan melakukan penggantian *password User ID*

secara berkala. Kebijakan ini bertujuan untuk mengurangi risiko akses tidak sah terhadap informasi medis, baik dari internal maupun eksternal rumah sakit.

Terdapat berbagai alasan mendasar yang memperkuat pentingnya kebijakan penggantian *password* ini. Penggunaan *password* yang terus-menerus tanpa pembaruan berkala dapat meningkatkan potensi kebocoran data, baik melalui peretasan digital maupun kelalaian pengguna. Oleh karena itu, rumah sakit harus menerapkan prosedur pengamanan tambahan, seperti pembatasan akses ke sistem informasi kesehatan, penggunaan *User ID* yang unik, serta pencegahan akses fisik ke data rekam medis berbasis kertas maupun elektronik. Tindakan ini juga dapat diperkuat dengan tanda atau rambu yang menandai area terbatas untuk mencegah pihak yang tidak berwenang memasuki ruang kerja atau sistem tertentu. Penelitian ini dilakukan dengan pendekatan kualitatif melalui wawancara terhadap petugas rekam medis di RS Hermina Arcamanik. Wawancara tersebut memuat tujuh pertanyaan utama yang berfokus pada kebijakan penggantian *password User ID*. Aspek-aspek yang digali meliputi faktor-faktor yang mempengaruhi tingkat kepatuhan pegawai terhadap kebijakan tersebut, sejauh mana kebijakan itu efektif dalam menjaga keamanan data pasien, serta tindakan- tindakan preventif yang perlu diambil setelah proses penggantian *password* dilakukan untuk memastikan keamanan akun tetap terjaga. Hasil wawancara menunjukkan bahwa keamanan data rekam medis elektronik sangat vital, tidak hanya untuk melindungi privasi pasien, tetapi juga untuk mencegah potensi penyalahgunaan informasi yang dapat merugikan pasien secara pribadi maupun menurunkan tingkat kepercayaan publik terhadap institusi rumah sakit. Dengan demikian, rumah sakit perlu terus mengembangkan kebijakan keamanan informasi yang adaptif terhadap perkembangan teknologi dan memperkuat kesadaran serta kedisiplinan seluruh staf dalam menerapkan protokol perlindungan data.

Kebijakan penggantian *password* secara berkala terbukti efektif dalam menjaga keamanan data rekam medis. Dengan mengganti *password* secara rutin, risiko akses yang tidak sah oleh pihak yang telah memperoleh *password* lama dapat diminimalisir. Jika terjadi kebocoran data, kebijakan ini dapat mengurangi dampak negatif karena *password* yang bocor akan segera menjadi tidak valid setelah batas waktu yang ditentukan.

Kepatuhan pengguna terhadap kebijakan ini dipengaruhi oleh berbagai faktor, termasuk kesadaran akan pentingnya keamanan data, kemudahan dalam mengubah *password,* sanksi yang diterapkan untuk pelanggaran, *human error*, serta ketertiban dalam pengelolaan SDM. Faktor-faktor ini dapat memengaruhi tingkat keberhasilan implementasi kebijakan tersebut. Pergantian *User ID* dalam beberapa bulan terakhir disebabkan oleh sejumlah faktor, umumnya terkait dengan upaya meningkatkan keamanan dan respons terhadap insiden keamanan. Salah satu faktor yang menyebabkan pergantian *User ID* adalah beban kerja yang tinggi pada SDM. Ketika terjadi pergantian *shift*, terkadang SDM lupa untuk *logout* dari *User ID* mereka, yang dapat menimbulkan risiko keamanan yang serius, terutama dalam konteks data rekam medis yang sensitif. Dengan adanya kebijakan *logout* otomatis dan pengawasan terhadap penggunaan *User ID*, diharapkan dapat meminimalkan risiko akibat kelalaian seperti ini.

Sistem RME juga dilengkapi dengan fitur pemberitahuan otomatis yang mengingatkan pengguna untuk mengganti *password* sebelum batas waktu yang ditentukan. Hal ini memberi pengguna waktu yang cukup untuk mengubah *password* dengan nyaman. Selain itu, ketika mengganti *password*, pengguna harus mematuhi persyaratan tertentu,

seperti panjang minimal karakter dan kombinasi huruf, angka, serta simbol, untuk memastikan tingkat keamanan yang lebih tinggi.

Privasi dan keamanan data rekam medis harus dijaga dengan ketat untuk mencegah penyalahgunaan informasi medis yang bisa membahayakan pasien. Oleh karena itu, perlindungan data yang baik mencakup pengelolaan data pasien melalui proses pengumpulan yang terkontrol, menjaga kualitas data, dan mengontrol akses ke data tersebut. Kebijakan keamanan seperti enkripsi, *logout* otomatis, serta penggunaan *username* dan *password* yang kuat, sangat penting untuk memastikan bahwa hanya pihak yang berwenang yang dapat mengakses sistem. Mengingat ancaman dari kesalahan manusia yang sering terjadi, penting untuk tidak hanya mengandalkan teknologi, tetapi juga meningkatkan kesadaran dan pelatihan keamanan bagi seluruh staf rumah sakit untuk meminimalkan risiko kesalahan manusia. Sistem juga perlu dilengkapi dengan mekanisme *logout* otomatis yang akan keluar dari sistem jika tidak ada aktivitas dalam jangka waktu tertentu. Ini untuk mengurangi risiko penyalahgunaan *User ID* dan melindungi data pasien dari akses yang tidak sah. Kebijakan privasi yang ketat juga diterapkan untuk melindungi informasi medis dan memastikan bahwa hanya pihak yang berwenang yang dapat mengakses data tersebut, meningkatkan kepercayaan pasien terhadap sistem kesehatan elektronik yang diterapkan.

Penerapan kebijakan penggantian *password* secara berkala terbukti menjadi salah satu upaya strategis dalam menjaga keamanan sistem RME di rumah sakit. Dengan memperbarui *password* secara rutin, risiko akses tidak sah dari pihak yang tidak berwenang dapat ditekan. Jika suatu *password* sempat bocor, sistem penggantian berkala akan secara otomatis membuat informasi yang diperoleh menjadi tidak lagi valid, sehingga potensi kerugian akibat kebocoran data dapat diminimalkan. Namun, efektivitas kebijakan ini sangat bergantung pada tingkat kepatuhan pengguna.

Beberapa faktor yang memengaruhi kepatuhan tersebut antara lain yaitu tingkat pemahaman terhadap pentingnya keamanan data, kemudahan dalam proses pergantian *password*, konsistensi penerapan sanksi terhadap pelanggaran, serta manajemen sumber daya manusia yang tertib. Selain itu, kesalahan manusia (*human error*) dan beban kerja yang tinggi juga turut memengaruhi keberhasilan kebijakan ini di lapangan. Pergantian *User ID* yang terjadi dalam beberapa bulan terakhir di RS Hermina Arcamanik umumnya dipicu oleh peningkatan upaya keamanan serta reaksi terhadap insiden keamanan yang pernah terjadi. Salah satu penyebab utama adalah kelalaian pengguna saat pergantian *shift* kerja. Dalam situasi sibuk, pengguna sering lupa melakukan *logou*t dari akun masing-masing, sehingga membuka peluang terjadinya penyalahgunaan data oleh pihak lain yang mengakses perangkat yang sama.

Sebagai bentuk pencegahan, penggunaan sistem *logout* otomatis sangat penting untuk mengatasi risiko tersebut. Ketika tidak ada aktivitas selama periode tertentu, sistem akan secara otomatis keluar dari akun, sehingga keamanan tetap terjaga meskipun pengguna lupa *logout* secara manual.

Sistem RME yang diterapkan juga telah dilengkapi dengan fitur notifikasi otomatis yang mengingatkan pengguna untuk mengganti *password* sebelum masa aktifnya habis. Proses pergantian ini dilakukan dengan ketentuan keamanan tertentu, seperti panjang karakter minimum, penggunaan kombinasi huruf besar, huruf kecil, angka, dan simbol. Tujuannya adalah untuk memastikan bahwa *password* yang digunakan kuat dan sulit untuk ditebak, sehingga lebih aman dari potensi peretasan.

Perlindungan terhadap privasi data pasien merupakan tanggung jawab penting bagi setiap institusi kesehatan. Informasi medis yang disalahgunakan tidak hanya dapat merugikan pasien secara pribadi, tetapi juga berpotensi menurunkan tingkat kepercayaan masyarakat terhadap sistem layanan kesehatan digital. Oleh karena itu, rumah sakit perlu melakukan pengelolaan data secara menyeluruh mulai dari proses input, penyimpanan, pemeliharaan integritas data, hingga pengaturan akses yang ketat. Meskipun teknologi menjadi tulang punggung pengamanan data, manusia tetap menjadi titik rawan utama dalam sistem informasi. Banyak pelanggaran data terjadi bukan karena kecanggihan teknologi, melainkan karena kelalaian atau kurangnya kesadaran staf pengguna sistem. Oleh karena itu, untuk mengoptimalkan keamanan sistem RME dan meminimalkan risiko pelanggaran data dibutuhkan pelatihan dan peningkatan kesadaran tentang keamanan data perlu dilaksanakan secara berkala untuk seluruh tenaga kerja, baik medis maupun administratif. Selain itu diperlukan peninjauan efektivitas kebijakan dan sistem keamanan secara berkala agar dapat menyesuaikan dengan dinamika teknologi dan kebutuhan rumah sakit.

Kesimpulan

Rumah sakit sebagai institusi pelayanan kesehatan memiliki tanggung jawab besar dalam menjaga keamanan dan kerahasiaan data pasien, terutama dengan semakin berkembangnya penggunaan RME. Penerapan kebijakan penggantian *password* secara berkala terbukti efektif dalam mengurangi risiko akses tidak sah dan kebocoran data pasien. Namun, keberhasilan kebijakan ini sangat bergantung pada tingkat kepatuhan pengguna yang dipengaruhi oleh faktor kesadaran, kemudahan penggantian *password*, serta disiplin dan manajemen sumber daya manusia.

Tantangan yang muncul seperti kelalaian pengguna dalam *logout* saat pergantian *shift* dan risiko *human error* dapat diminimalkan melalui sistem *logout* otomatis dan pengingat penggantian *password* yang terintegrasi. Selain itu, penerapan standar keamanan *password* yang ketat sangat penting untuk memperkuat sistem autentikasi.

Perlindungan data rekam medis bukan hanya soal teknologi, tetapi juga memerlukan peningkatan kesadaran dan pelatihan berkelanjutan bagi seluruh staf rumah sakit. Dengan demikian, rumah sakit dapat memastikan integritas, kerahasiaan, dan ketersediaan data pasien terjaga dengan baik, sekaligus memenuhi ketentuan regulasi yang berlaku.

Upaya pengelolaan keamanan informasi yang komprehensif dan adaptif terhadap perkembangan teknologi menjadi kunci utama dalam meningkatkan kepercayaan masyarakat terhadap layanan kesehatan digital dan menjaga reputasi institusi rumah sakit Dalam rangka menjaga keamanan akses sistem RME, diterapkan prosedur standar untuk penggantian *password* pengguna. Proses dimulai saat pengguna mengajukan permintaan penggantian *password* melalui saluran resmi, baik secara tertulis maupun melalui sistem tiket. Informasi dasar seperti nama, identitas pegawai, dan alasan penggantian wajib disertakan. Tim Teknologi Informasi kemudian melakukan verifikasi identitas berdasarkan data yang tersedia. Jika verifikasi berhasil, *password* di-reset dan *password* sementara dikirimkan ke alamat email atau kontak resmi pengguna. Setelah itu, pengguna diminta segera mengganti *password* sementara dengan *password* baru yang bersifat pribadi. Selain itu, sistem RME menyediakan fitur penggantian *password* secara mandiri melalui pengaturan akun, dengan syarat autentikasi ulang. *Password* yang digunakan harus memenuhi ketentuan keamanan tertentu, seperti panjang minimal dan kombinasi karakter.

Dalam kondisi tertentu, seperti dugaan pelanggaran keamanan, akun pengguna dapat dinonaktifkan sementara dan dilakukan audit aktivitas untuk memastikan tidak terjadi penyalahgunaan data. Seluruh proses penggantian dicatat dalam log sistem sebagai bagian dari mekanisme pengawasan dan evaluasi.

Ucapan Terima Kasih

Pada kesempatan ini, penulis mengucapkan terima kasih yang sebesar-besarnya kepada pihak RS Hermina Arcamanik yang telah memberikan izin dan kesempatan untuk melakukan penelitian ini. Ucapan terima kasih juga ditujukan kepada seluruh petugas rekam medis, tenaga medis, serta staf rumah sakit yang telah meluangkan waktu dan memberikan informasi berharga selama proses pengumpulan data berlangsung.

Penulis juga menyampaikan rasa terima kasih yang mendalam kepada dosen pembimbing, Ibu Sali Setiatin, A.Md.Perkes., S.ST., M.MRS., CPS yang telah memberikan arahan, dukungan, dan motivasi selama penyusunan jurnal ini dan Bapak Indra selaku Pembimbing Lapangan atas bimbingan dan arahan yang diberikan selama proses penelitian. Semoga hasil penelitian ini dapat memberikan kontribusi positif dalam peningkatan keamanan data serta kualitas pelayanan di RS Hermina Arcamanik.

Daftar Pustaka

Camila, C. N., & Anggraini, D. T. (2025). Implementasi Rekam Medis Elektronik sebagai Strategi Digitalisasi Pelayanan Kesehatan, (April).

Mudasir. (2024). *Wawancara dan Observasi*. *Pembangunan DAM*.

Nugroho, S. J. (2025). Digitalisasi : Solusi Efisiensi Pelayanan Rumah Sakit Masa Kini, (January).

PP RI NO 71, 2019. (2019). Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik. *Media Hukum*, *7*(2), 70.

Rahma, A., & Suryani, A. I. (2024). Analisis Penggantian Password User Id Dalam Sistem Rekam Medis Elektronik Guna Menjaga Keamanan Data Rekam Medis Di Rumah Sakit Hermina Arcamanik.

Romdona, S., Junista, S., & Gunawan, ahmad. (n.d.). Teknik Pengumpulan Data, *3*(1), 39–47.

Setiatin, Seli & Kusuma, S. (2025). Pengaruh Data Statistik terhadap Aplikasi EMR Rumah Sakit Hermina Arcamanik Kota Bandung, (301), 97104.

Sugiyono. (2020). *Metodologi Penelitian Kuantitatif, Kualitatif dan R & D*.

UU Nomor 17 Tahun 2007. (2007).

Wilar, Y. A., Yuliawan, K., & Natsir, A. A. (2023). Analisis Keamanan Sistem Manajemen Informasi Rumah Sakit Umum Daerah Nabire. *MAHESA : Malahayati Health Student Journal*, *3*(10), 3365–3374. https://doi.org/10.33024/mahesa.v3i10.11246