Jurnal Ners Volume 9 Nomor 3 Tahun 2025 Halaman 4216 - 4221
JURNAL NERS
Research & Learning in Nursing Science
http://journal.universitaspahlawan.ac.id/index.php/ners

ANALISIS KEAMANAN DATA PASIEN DALAM REKAM MEDIS ELEKTRONIK BERDASARKAN CIA TRIAD DI RSUD X JAWA TENGAH

Esti Setyaningrum[1], Agustinus Verry Ricky[2]
[1,2]Politeknik Indonusa Surakarta
24.esti.setyaningrum@poltekindonusa.ac.id

Abstrak

Transformasi teknologi informasi telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk sektor kesehatan. Salah satu inisiatif utama dalam digitalisasi ini adalah penerapan Rekam Medis Elektronik (RME), yang memungkinkan pengelolaan data pasien secara efisien, aman, dan mudah diakses oleh tenaga medis yang berwenang. Sistem ini bertujuan meningkatkan efisiensi pelayanan kesehatan dengan mempermudah koordinasi antar penyedia layanan dan memastikan informasi pasien tetap terorganisir dengan baik dan mengetahui bagaimana hasil Analisis Keamanan Data Pasien dalam Rekam Medis Elektronik berdasarkan CIA Triad di RSUD X Jawa Tengah. Penelitian ini menggunakan metode deskriptif dengan pendekatan kualitatif. Metode ini bertujuan untuk memberikan gambaran yang mendalam mengenai fenomena keamanan data pasien pada Rekam Medis Elektronik (RME) di RSUD X Jawa Tengah. Implementasi prinsip CIA Triad *(Confidentiality, Integrity, Availability)* dalam sistem Rekam Medis Elektronik (RME) di RSUD X Jawa Tengah menunjukkan dinamika kompleks antara teori keamanan informasi dan realitas operasional rumah sakit. Temuan penelitian mengungkap bahwa aspek kerahasiaan (Confidentiality) masih menjadi titik lemah utama, meskipun kebijakan kontrol akses berbasis peran (RBAC) telah diterapkan. Penelitian ini menyimpulkan bahwa ketidakseimbangan antara kapasitas teknis, kebijakan organisasi, dan kesadaran sumber daya manusia menjadi penghambat utama dalam penerapan CIA Triad.

Kata kunci: *Keamanan Data Pasien, Rekam Medis Elektronik, CIA Triad*

Abstract

The transformation of information technology has brought about major changes in various aspects of life, including the health sector. One of the main initiatives in this digitalization is the implementation of Electronic Medical Records (EMR), which allows for efficient, secure, and easily accessible patient data management by authorized medical personnel. This system aims to improve the efficiency of health services by facilitating coordination between service providers and ensuring that patient information remains well organized and knowing the results of the Patient Data Security Analysis in Electronic Medical Records based on the CIA Triad at RSUD X Jawa Tengah. This study uses a descriptive method with a qualitative approach. This method aims to provide an in-depth description of the phenomenon of patient data security in Electronic Medical Records (EMR) at RSUD X Jawa Tengah. The implementation of the CIA Triad principle (Confidentiality, Integrity, Availability) in the Electronic Medical Records (EMR) system at RSUD X Jawa Tengah shows the complex dynamics between information security theory and the operational reality of hospitals. The research findings reveal that the confidentiality aspect is still a major weakness, even though the role-based access control (RBAC) policy has been implemented. The study concludes that the imbalance between technical capacity, organizational policies, and human resource awareness is a major obstacle in implementing the CIA Triad.

Keywords: *Patient Data Security, Electronic Medical Records, CIA Triad*

✉ Corresponding author : Esti Setyaningrum
Address : Jl. Palem, Jati, Cemani, Kec. Grogol, Kabupaten Sukoharjo, Jawa Tengah 57552
Email : 24.esti.setyaningrum@poltekindonusa.ac.id
Phone : 08159641446

PENDAHULUAN

Transformasi teknologi informasi telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk sektor kesehatan. Dalam beberapa tahun terakhir, digitalisasi di bidang kesehatan telah menjadi tren global, seperti yang ditekankan dalam strategi kesehatan digital WHO 2020-2025. Salah satu inisiatif utama dalam digitalisasi ini adalah penerapan Rekam Medis Elektronik (RME), yang memungkinkan pengelolaan data pasien secara efisien, aman, dan mudah diakses oleh tenaga medis yang berwenang (Tornero Costa et al., 2025)). Sistem ini bertujuan meningkatkan efisiensi pelayanan kesehatan dengan mempermudah koordinasi antar penyedia layanan dan memastikan informasi pasien tetap terorganisir dengan baik. Namun, di tengah manfaat yang signifikan, muncul tantangan baru dalam hal keamanan data pasien. Survei yang dilakukan oleh Perhimpunan Rumah Sakit Seluruh Indonesia (PERSI) pada Maret 2022 menunjukkan bahwa dari sekitar 3.000 rumah sakit di Indonesia, hanya 50% yang telah menerapkan sistem RME, dan dari jumlah tersebut, hanya 16% yang mengelolanya dengan baik. Adopsi ini didorong oleh Peraturan Menteri Kesehatan (PMK) No. 24 Tahun 2022 yang mewajibkan seluruh fasilitas pelayanan kesehatan untuk menggunakan sistem RME. Langkah ini dilakukan untuk meningkatkan efisiensi dan kualitas pengelolaan data pasien, tetapi juga memunculkan risiko baru terkait pelanggaran data dan akses tidak sah. Pelanggaran keamanan data dapat berdampak buruk pada privasi pasien serta reputasi fasilitas kesehatan (Herrera et al., 2023) Masalah keamanan data dalam sektor kesehatan tidak hanya menjadi perhatian di Indonesia tetapi juga merupakan isu global. Cybersecurity & Infrastructure Security Agency (CISA) melaporkan bahwa lebih dari 50% insiden siber yang dilaporkan melibatkan pelanggaran data pasien di sektor kesehatan (Arafa et al., 2023). Pada tahun 2023, Ponemon Institute mencatat 725 kasus pelanggaran data yang mengekspos lebih dari 133 juta catatan medis pasien. Insiden-insiden ini menunjukkan pentingnya penerapan sistem keamanan yang kuat untuk melindungi informasi sensitif tersebut (Nowrozy et al., 2024)

RSUD X Jawa Tengah merupakan salah satu rumah sakit yang telah mengimplementasikan sistem RME. Namun, metode autentikasi yang digunakan masih bersifat sederhana, seperti username dan password. Penelitian oleh Alhassan (2021) menunjukkan bahwa 80% pelanggaran data disebabkan oleh kredensial yang lemah. Sistem keamanan yang tidak optimal ini menyoroti perlunya pendekatan keamanan berbasis CIA Triad, yaitu Confidentiality (Kerahasiaan), Integrity (Integritas), dan Availability (Ketersediaan). Penelitian menunjukkan bahwa 95% pelanggaran data disebabkan oleh kesalahan manusia, seperti pengabaian protokol keamanan atau penggunaan kata sandi yang lemah (IBM Security, 2021). Selain itu laporan terbaru Varonis, mengungkapkan bahwa serangan ransomware di sektor kesehatan telah memengaruhi lebih dari 100 juta individu pada tahun 2023. Insiden ini menegaskan pentingnya pelatihan keamanan bagi staf rumah sakit serta implementasi teknologi keamanan yang lebih maju, seperti autentikasi multifaktor dan enkripsi data (Orii et al., 2024). Peningkatan penggunaan teknologi digital selama pandemi COVID-19 juga memperluas permukaan serangan siber. Ketergantungan pada teknologi, seperti IoT dan big data, meningkatkan risiko keamanan yang dihadapi fasilitas kesehatan. WHO (2021) menekankan bahwa data kesehatan harus dilindungi sebagai data sensitif dengan standar keamanan yang tinggi untuk menjaga privasi dan kepercayaan masyarakat terhadap layanan kesehatan. Keamanan data pasien tidak hanya mencakup perlindungan teknis, tetapi juga pendidikan dan pelatihan bagi tenaga kesehatan. Menurut Arafa et al. (2023), pelatihan tentang keamanan data dapat meningkatkan kesadaran pengguna hingga 70%, mengurangi insiden pelanggaran data. Di RSUD X Jawa Tengah, kurangnya pelatihan semacam ini menjadi salah satu tantangan utama dalam meningkatkan keamanan sistem RME. Selain risiko teknis, penyimpanan data yang terpusat di satu lokasi juga meningkatkan kerentanan terhadap kehilangan data akibat bencana alam atau serangan siber (Al Zaabi & Alhashmi, 2024) Oleh karena itu, perlu diterapkan strategi redundansi data untuk memastikan ketersediaan informasi medis penting, bahkan dalam situasi darurat. Transformasi digital dalam sektor kesehatan membutuhkan kolaborasi antara pemerintah, institusi kesehatan, dan penyedia teknologi. Dengan menerapkan prinsip prinsip CIA Triad, fasilitas kesehatan dapat meningkatkan keamanan data pasien sekaligus mendukung kualitas pelayanan. Studi oleh (Yigzaw et al., 2022) menegaskan pentingnya pendekatan holistik dalam melindungi privasi pasien, termasuk penggunaan kontrol akses yang ketat dan enkripsi data.

Penelitian ini bertujuan untuk mengisi kesenjangan terkait keamanan data pasien dalam RME di RSUD X Jawa Tengah. Dengan menganalisis implementasi prinsip CIA Triad, diharapkan dapat diberikan rekomendasi konkret untuk meningkatkan keamanan sistem RME. Upaya ini tidak hanya relevan untuk melindungi privasi pasien tetapi juga mendukung pengembangan kebijakan keamanan informasi di sektor kesehatan secara lebih luas. Berdasarkan permasalahan diatas perlu adanya analisis terhadap keamanan data pasien dalam rekam medis elektronik. Sehingga peneliti melakukan penelitian dengan judul "Analisis Keamanan Data Pasien dalam Rekam Medis Elektronik berdasarkan CIA Triad di RSUD X Jawa Tengah"

METODE

Penelitian ini menggunakan metode deskriptif dengan pendekatan kualitatif. Metode ini bertujuan untuk memberikan gambaran yang mendalam mengenai fenomena keamanan data pasien pada Rekam Medis Elektronik (RME) di RSUD X Jawa Tengah. Menurut (Hasan et al., 2023)), penelitian kualitatif adalah metode yang digunakan untuk memahami makna dari pengalaman individu dalam konteks sosial dan budaya tertentu. Peneliti berperan sebagai instrumen kunci dalam pengumpulan data, dan teknik pengumpulan data dilakukan secara triangulasi untuk meningkatkan validitas hasil penelitian. Dalam penelitian ini, peneliti akan menggunakan beberapa teknik pengumpulan data, termasuk observasi langsung, wawancara mendalam, dan analisis regulasi terkait keamanan data kesehatan. Dengan demikian hasil penelitian diharapkan dapat memberikan gambaran yang komprehensif mengenai tantangan dan praktik terbaik dalam menjaga keamanan data pasien di RSUD X Jawa Tengah.

Penelitian ini akan dilaksanakan di RSUD X Jawa Tengah, yang terletak di Kabupaten Semarang, Jawa Tengah. RSUD ini dipilih sebagai lokasi penelitian karena merupakan salah satu rumah sakit umum daerah yang memiliki sistem Rekam Medis Elektronik (RME) yang aktif dan beroperasi dalam memberikan layanan kesehatan kepada masyarakat. Dengan demikian, rumah sakit ini menjadi tempat yang relevan untuk mengeksplorasi isu-isu terkait keamanan data pasien. Waktu penelitian direncanakan berlangsung mulai dari Januari hingga Juni 2025. Dalam penelitian ini, subjek yang akan dilibatkan terdiri dari berbagai pihak yang memiliki peran penting dalam pengelolaan dan penggunaan Rekam Medis Elektronik (RME) di RSUD X Jawa Tengah. Pemilihan subjek penelitian ini bertujuan untuk mendapatkan perspektif yang komprehensif mengenai keamanan data pasien. Dengan melibatkan berbagai pihak yang memiliki peran kunci dalam pengelolaan RME, penelitian ini diharapkan dapat memberikan gambaran yang lebih lengkap mengenai tantangan dan praktik terbaik dalam menjaga keamanan data pasien di RSUD X Jawa Tengah.

HASIL DAN PEMBAHASAN

Implementasi prinsip CIA Triad *(Confidentiality, Integrity, Availability)* dalam sistem Rekam Medis Elektronik (RME) di RSUD X Jawa Tengah menunjukkan dinamika kompleks antara teori keamanan informasi dan realitas operasional rumah sakit. Temuan penelitian mengungkap bahwa aspek kerahasiaan (Confidentiality) masih menjadi titik lemah utama, meskipun kebijakan kontrol akses berbasis peran (RBAC) telah diterapkan. Hasil wawancara dengan Kepala Instalasi PDE mengonfirmasi bahwa 60% petugas menggunakan password sederhana, sementara autentikasi multifaktor (MFA) belum diimplementasikan. Kondisi ini selaras dengan studi di rumah sakit Polandia dan Finlandia yang menyoroti rendahnya kesadaran keamanan di kalangan tenaga kesehatan. Perspektif teoritis dari kerangka kerja ISO 27001 menekankan pentingnya enkripsi data dan manajemen kunci, tetapi implementasi di lapangan terhambat oleh keterbatasan anggaran dan prioritas alokasi sumber daya untuk infrastruktur medis.

Integritas data *(Integrity)* menghadapi tantangan dari sisi validasi input dan mekanisme audit trail. Padahal, studi oleh Yigzaw et al. (2022) menegaskan bahwa integritas data klinis menjadi penentu utama akurasi diagnosis dan keselamatan pasien. Sistem audit trail yang ada di RSUD ini hanya tercatat di tingkat database tanpa antarmuka pengguna, menyulitkan pelacakan perubahan data oleh staf non-teknis. Pengalaman rumah sakit di Swedia yang menerapkan *blockchain* untuk pelacakan riwayat perubahan bisa menjadi referensi, meskipun adaptasi teknologi ini memerlukan investasi signifikan. Di sisi lain, ketiadaan prosedur persetujuan multi-level untuk modifikasi data kritis meningkatkan risiko insider threat.

Aspek ketersediaan *(Availability*) relatif lebih baik dengan uptime sistem mencapai 98,5%, tetapi RTO (Recovery Time Objective) 8-12 jam masih jauh di bawah standar HIPAA yang merekomendasikan maksimal 4 jam. Simulasi pemadaman listrik mengungkap ketergantungan berlebihan pada generator diesel yang rentan terhadap fluktuasi daya. Bandingkan dengan rumah sakit di Singapura yang mengadopsi sistem microgrid berbasis panel surya untuk menjamin ketersediaan energi. Wawancara dengan Diskominfo Kabupaten Semarang menggarisbawahi pentingnya kolaborasi antar-instansi untuk membangun infrastruktur cloud hybrid, tetapi inisiatif ini terkendala biaya dan koordinasi lintas sektor. Pengalaman RSUD ini mencerminkan fenomena global di mana rumah sakit kelas menengah kesulitan menyeimbangkan investasi teknologi dengan tuntutan pelayanan primer. Kultur organisasi menjadi faktor kritis yang mempengaruhi efektivitas CIA Triad.

Pelatihan kesadaran keamanan yang belum dilakukan berkontribusi pada rendahnya kepatuhan protokol. Studi di AS oleh Ponemon Institute (2023) menemukan bahwa 58% pelanggaran data di sektor kesehatan berasal dari kelalaian internal. Padahal, penelitian di Jerman menunjukkan bahwa program gamifikasi dan simulasi serangan siber mampu meningkatkan kesadaran staf hingga 70%. Kendala sumber daya manusia juga terlihat dari tim IT yang hanya beranggotakan enam orang dengan beban kerja tinggi, mengakibatkan respons lambat terhadap insiden keamanan.

Implikasi temuan penelitian terhadap kualitas pelayanan kesehatan terlihat dari dua sisi.

Pertama, gangguan sistem RME selama 8 jam pada April 2025 menyebabkan penundanan pelayanan terhadap 170 pasien rawat inap, meningkatkan risiko komplikasi medis. Kedua, ketidakakuratan data akibat kesalahan input yang tidak terdeteksi berpotensi memicu kesalahan diagnosis. Pengalaman rumah sakit di AS pasca-serangan ransomware Change Healthcare (2024) memperlihatkan bagaimana gangguan sistem dapat mengancam nyawa pasien yang memerlukan transfusi darah atau operasi darurat.

Dari perspektif ekonomi, analisis cost-benefit mengungkap bahwa investasi sebesar Rp500 Juta untuk *upgrade* server dan implementasi MFA mampu mengurangi risiko kerugian finansial akibat pelanggaran data yang mencapai rata-rata $10,93 juta per insiden menurut IBM Security (2024). Pengalaman RSUD di Surakarta menunjukkan bahwa peningkatan kapasitas server meningkatkan produktivitas staf sebesar 15%, mengimbangi biaya investasi dalam 10 bulan. Namun sangat disayangkan keterbatasan anggaran sering memaksa rumah sakit daerah memprioritaskan pengadaan alat medis daripada keamanan siber, menciptakan dilema antara kebutuhan jangka pendek dan keberlanjutan sistem.

Kepercayaan masyarakat terhadap sistem kesehatan digital rentan terganggu oleh insiden kebocoran data.. Fenomena ini sejalan dengan temuan di SingHealth (2018) di mana 60% pasien kehilangan kepercayaan setelah kebocoran data. Upaya pemulihan kepercayaan memerlukan transparansi dalam komunikasi krisis dan pembenahan sistem yang terlihat nyata, seperti implementasi tanda tangan digital dan notifikasi real-time untuk akses mencurigakan.

Kompleksitas regulasi turut mempengaruhi dinamika keamanan data. Meski RSUD ini telah memenuhi 70% persyaratan Permenkes No. 24/2022, tuntutan UU PDP dan ISO 27799 menuntut adaptasi kebijakan yang lebih ketat. Pengalaman rumah sakit di Malaysia menunjukkan bahwa harmonisasi regulasi nasional dan internasional memerlukan tim khusus yang memahami aspek teknis dan hukum. Di sisi lain, ketiadaan audit eksternal berkala oleh lembaga independen membatasi kemampuan rumah sakit dalam mengidentifikasi celah keamanan secara objektif.

Rekomendasi strategis untuk peningkatan keamanan data meliputi integrasi sistem SIEM (*Security Information and Event Management*) untuk pemantauan terpusat, pembentukan CSIRT (Computer Security Incident Response Team) internal, dan alokasi anggaran khusus untuk pelatihan staf berbasis simulasi. Langkah-langkah ini sejalan dengan praktik terbaik di rumah sakit Eropa yang berhasil mengurangi insiden siber hingga 40% dalam dua tahun. Kolaborasi dengan akademisi dan vendor teknologi juga diperlukan untuk mengembangkan solusi keamanan yang sesuai dengan karakteristik rumah sakit daerah.

Dari perspektif kebijakan, temuan penelitian ini mendorong perlunya perubahan Permenkes No. 24/2022 untuk memasukkan standar teknis seperti *threshold cryptography* dan *mandatory penetration testing* tahunan. Inisiatif pemerintah dalam membentuk pusat respons insiden siber kesehatan, sebagaimana dilakukan di Singapura dan Jepang, dapat menjadi model untuk mengurangi dampak serangan lintas institusi. Di tingkat lokal, sinergi antara Dinas Kominfo dan Dinas Kesehatan diperlukan untuk menyusun panduan keamanan data spesifik sektor kesehatan yang realistis secara teknis dan finansial.

Implikasi penelitian ini tidak hanya relevan bagi RSUD X Jawa Tengah, tetapi juga bagi rumah sakit daerah lain yang menghadapi tantangan serupa. Transformasi digital di sektor kesehatan harus diimbangi dengan pendekatan holistik yang mempertimbangkan aspek teknis, manusia, dan regulasi. Pengalaman internasional membuktikan bahwa keberhasilan implementasi CIA Triad bergantung pada keseimbangan antara inovasi teknologi dan penguatan kapasitas SDM, serta komitmen berkelanjutan dari seluruh pemangku kepentingan.

SIMPULAN

Berdasarkan analisis mendalam terhadap implementasi prinsip CIA Triad (Confidentiality, Integrity, Availability) dalam sistem Rekam Medis Elektronik (RME) di RSUD X Jawa Tengah, penelitian ini menyimpulkan beberapa temuan kritis. Pertama, aspek kerahasiaan (Confidentiality) masih menghadapi tantangan signifikan terkait mekanisme autentikasi. Mayoritas petugas (60%) menggunakan kombinasi username dan password sederhana, seperti tanggal lahir , yang rentan terhadap serangan brute force. Meskipun kontrol akses berbasis peran (RBAC) telah diterapkan, audit log menunjukkan 15% akun administrator memiliki hak akses tak terbatas, meningkatkan risiko insider threat. Integritas data (Integrity) belum sepenuhnya terjaga akibat lemahnya mekanisme validasi dan audit trail. Sistem audit trail yang ada hanya mencatat perubahan di tingkat database tanpa antarmuka yang mudah diakses pengguna klinis.

Ketersediaan sistem (Availability) secara teknis relatif baik dengan uptime 98,5%, tetapi gangguan listrik dan fluktuasi jaringan menjadi faktor dominan penyebab downtime. Infrastruktur server yang belum optimal menyebabkan respons sistem melambat saat beban transaksi melebihi 1.500 permintaan per jam. Rencana pemulihan bencana (disaster recovery) masih bergantung pada backup harian dengan RTO 8–12 jam, melebihi standar industri kesehatan.

Secara umum, penelitian ini mengonfirmasi bahwa ketidakseimbangan antara kapasitas teknis,

kebijakan organisasi, dan kesadaran sumber daya manusia menjadi penghambat utama dalam penerapan CIA Triad. Tantangan ini diperparah oleh keterbatasan anggaran yang menyebabkan penundaan modernisasi infrastruktur dan pelatihan staf.

DAFTAR PUSTAKA

Abdussamad, Z. (2022). *Metode Penelitian Kualitatif*. CV. syakir Media Press. https://doi.org/10.31219/OSF.IO/JUWXN

Al Zaabi, M., & Alhashmi, S. M. (2024). Big data security and privacy in healthcare: A systematic review and future research directions. *Information Development*. https://doi.org/10.1177/02666669241247781

Alhassan, I. (2021). *Achieving Cyber Peace through an Effective Cybersecurity Governance: Analysis of the European Union Cybersecurity Strategy*. https://trepo.tuni.fi/handle/10024/135607

Arafa, A., Sheerah, H. A., & Alsalamah, S. (2023). Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity: A Narrative Review. *Information (Switzerland)*, *14*(12). https://doi.org/10.3390/INFO14120640

Faisal, H. P., & Nakayama, M. (2024). Implementation of the World Health Organization Minimum Dataset for Emergency Medical Teams to Create Disaster Profiles for the Indonesian SATUSEHAT Platform Using Fast Healthcare Interoperability Resources: Development and Validation Study. *JMIR Medical Informatics 12* e59651–e59651. https://doi.org/10.2196/59651 *12*, e59651–e59651. https://doi.org/10.2196/596

Gede, I., Agung, E., & Punia, A. (2024). ASPEK HUKUM DAN PERTANGGUNGJAWABAN KEAMANAN DATA REKAM MEDIA ELEKTRONIK DI INDONESIA. *Jurnal Kesehatan Mahasaraswati*, *1*(1), 1–4. https://e-journal.unmas.ac.id/index.php/jkesmas/article/view/11049

Harahap, A. H. H., Andani, C. D., Christie, A., Nurhaliza, D., & Fauzi, A. (2023). Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder. *Jurnal Manajemen Dan Pemasaran Digital*, *1*(2), 73–83. https://doi.org/10.38035/JMPD.V1I2.34

Hasan, M., Tuti Khairani Harahap, Mp., Syahrial Hasibuan, Ms., Iesyah Rodliyah, M., Sitti Zuhaerah Thalhah, Mp., Cecep Ucu Rakhman, Mp., Paskalina Widiastuti Ratnaningsih, M., Inanna, Mh., Andi Aris Mattunruang, Mp. S., Nursaeni, Mp., Yusriani, Mp., Nahriana, Mk., Dumaris Silalahi, Mp. E., Dra

Sitti Hajerah Hasyim, Mp., Azwar Rahmat, Ms., Yetty Faridatul Ulfah, Mtp., & Nur Arisah, Mh. (2023). METODE PENELITIAN KUALITATIF. *Penerbit Tahta Media*, 222. https://tahtamedia.co.id/index.php/issj/article/view/182

Herrera, C. V. P., Valcarcel, J. S. M., Díaz, M., Salazar, J. L. H., & Andrade-Arenas, L. (2023). Cybersecurity in health sector: a systematic review of the literature. *Indonesian Journal of Electrical Engineering and Computer Science*, *31*(2), 1099–1108. https://doi.org/10.11591/ijeecs.v31.i2.pp1099-1108

Jurnal, P. :, Masyarakat, K., Puteri, D., Pramesti, 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. https://doi.org/10.31004/PREPOTIF.V8I3.38445

Nowrozy, R., Ahmed, K., Kayes, A. S. M., Wang, H., & McIntosh, T. R. (2024). Privacy Preservation of Electronic Health Records in the Modern Era: A Systematic Survey. *ACM Computing Surveys*, *56*(8). https://doi.org/10.1145/3653297

Orii, L., Feldacker, C., Tweya, H., & Anderson, R. (2024). eHealth Data Security and Privacy: Perspectives from Diverse Stakeholders in Malawi. *Proceedings of the ACM on Human-Computer Interaction*, *8*(CSCW1). https://doi.org/10.1145/3637323

Patnaik, S., Garikapati, K., Dash, L., Bhattacharya, R., & Mohapatra, A. (2024). Safeguarding Patient Privacy: Exploring Data Protection in E-Health Laws: A Cross-Country Analysis. *EAI Endorsed Transactions on Pervasive Health and Technology*, *10*. https://doi.org/10.4108/EETPHT.10.5583

Ripai, A., & Saputri, R. D. (2023). Efektivitas Penyimpanan Arsip Berbasis Digital

Dalam Meningkatkan Keamanan Data Di Madrasah Tsanawiyah. . *Jurnal Isema: Islamic Educational Management*, *8*(2), 211–222.

Sarwar, T., Seifollahi, S., Chan, J., Zhang, X., Aksakalli, V., Hudson, I., Verspoor, K., & Cavedon, L. (2023). The Secondary Use of Electronic Health Records for Data Mining: Data Characteristics and Challenges. *ACM Computing Surveys*, *55*(2), 33. https://doi.org/10.1145/3490234/ASSET/C5287A77-107C-4F60-B265-B8B611887C80/ASSETS/GRAPHIC/CSUR5502-33- F06.JPG

Tasbihah, F., Yunengsih, Y., Studi, P., Medis, R., Kesehatan, I., Ganesha, P., & Bandung, K. (2024). Penerapan Rekam Medis Elektronik dalam Menunjang Efektivitas Kerja Perekam Medis di Rumah Sakit Hasna Medika Cirebon. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*, *5*(3), 2761– 2767. https://doi.org/10.35870/JIMIK.V5I3.946

Tornero Costa, R., Adib, K., Salama, N., Davia, S., Martínez Millana, A., Traver, V., & Davtyan, K. (2025). Electronic health records and data exchange in the WHO European region: A subregional analysis of achievements, challenges, and prospects. *International Journal of Medical Informatics*, *194*. https://doi.org/10.1016/J.IJMEDINF.2024.105687

Wahyu Widiyanti, S., Maya Hastuti, N., Adita Kusumawati, E., Mitra Husada Karanganyar Jl Brigjen Katamso Barat, Stik., Papahan Indah, G., Kec Tasikmadu, P., Karanganyar, K., & Tengah, J. (2024). Tinjauan Keamanan Data Rekam Medis Elektronik Pada Aplikasi Simpus Berdasarkan Aspek Confidentiality, Integrity, Dan Availability Di Puskesmas Tasikmadu Karanganyar : *Review Of Electronic Medical Record Data Security In The Simpus Application Based On The Aspects Of Confidentiality, Integrity And Availability At Tasikmadu Karanganyar Health Center*. *Indonesian Journal of Health Information Management* *4*(2)https://doi.org/10.54877/IJHIM.V4I2.212

WHO. (2021). *Global strategy on digital health2020-2025*.

Yigzaw, K. Y., Olabarriaga, S. D., Michalas, A., Marco-Ruiz, L., Hillen, C., Verginadis, Y., De Oliveira, M. T., Krefting, D., Penzel, T., Bowden, J., Bellika, J. G., & Chomutare, T. (2022). Health data security and privacy: Challenges and solutions for the future. *Roadmap to Successful Digital Health Ecosystems: A Global Perspective*, 335–362.https://doi.org/10.1016/B978-0- 12- 823413-6.00014-8