Almufi Jurnal Sosial dan Humaniora (ASH)
Website: http://almufi.com/index.php/ASH
Email: almufi.ash@gmail.com

Analisis Hukum terhadap Cyber Crime dalam Rekam Medis Digital Militer (Studi Pendekatan UU TNI)

INFO PENULIS

Abd. Basir
Universitas Indonesia Timur
Abdbasir788@gmail.com

Ambo Esa
Universitas Indonesia Timur
Ambo.esa@uit.ac.id

Syawaluddin Boy
Universitas Indonesia Timur

INFO ARTIKEL

ISSN: 3046-8507
Vol. 3, No. 3, November 2026
http://almufi.com/index.php/ASH

© 2026 Almufi All rights reserved

Saran Penulisan Referensi:

Basir, A., Esa, A., Boy, S. (2026). Analisis Hukum terhadap Cyber Crime dalam Rekam Medis Digital Militer (Studi Pendekatan UU TNI). *Almufi Jurnal Sosial dan Humaniora, 3* (3), 128-135.

Abstrak

Transformasi digital dalam kesehatan militer melalui rekam medis elektronik, telemedicine, kecerdasan buatan, dan analitik data meningkatkan efisiensi serta kualitas pelayanan, tetapi juga menimbulkan risiko privasi dan keamanan siber. Rekam medis elektronik rentan terhadap pencurian, manipulasi, ransomware, dan kebocoran data akibat kesalahan manusia, sistem lama, serta kurangnya tenaga keamanan siber. Pada lingkungan militer, konektivitas perangkat medis semakin meningkatkan ancaman siber sehingga diperlukan perlindungan yang kuat tanpa mengurangi fungsi operasional. Di Indonesia, tingginya ancaman siber dan kasus kebocoran data menunjukkan pentingnya penguatan keamanan sistem elektronik, termasuk milik TNI. RME anggota TNI merupakan data sensitif yang dilindungi UU ITE, khususnya terkait larangan akses ilegal, pengungkapan rahasia, dan manipulasi data elektronik. Selain itu, UU No. 34 Tahun 2004 tentang TNI mewajibkan prajurit menjaga rahasia tentara. Pelanggaran dapat dikenai sanksi pidana, disiplin, maupun hukum militer. Sistem Pertahanan Kesehatan Nasional bertujuan mengintegrasikan sumber daya kesehatan militer dan sipil untuk menghadapi ancaman kesehatan serta memperkuat ketahanan nasional. Pelaksanaannya memerlukan sinergi, infrastruktur, regulasi, sumber daya, dan pembiayaan yang memadai. Penelitian ini merupakan penelitian hukum normatif. Hasil penelitian menunjukkan bahwa Kejahatan siber pada layanan kesehatan militer meliputi akses ilegal, manipulasi data medis, dan ransomware. Kerentanannya mencakup kelemahan SIMRS, keterbatasan infrastruktur, jaringan lambat, kata sandi lemah, serta ketidaklengkapan data medis yang dapat memengaruhi akurasi profil kesiapan tempur prajurit. Penanganan kejahatan siber rekam medis militer memiliki kekhususan berdasarkan UU No. 34 Tahun 2004 tentang TNI, karena rekam medis prajurit termasuk rahasia tentara. Kebocoran data dapat dikenai sanksi pidana, disiplin, dan peradilan militer karena berpotensi mengancam keamanan serta pertahanan negara.

Kata kunci: Cyber Crime, Rekam Medis Digital Militer, UU TNI.

Abstract

Digital transformation in military healthcare through electronic medical records, telemedicine, artificial intelligence, and data analytics improves efficiency and quality of care, but also creates privacy and cybersecurity risks. Electronic medical records are vulnerable to theft, manipulation, ransomware, and data breaches due to human error, outdated systems, and a shortage of cybersecurity personnel. In military environments, the increasing connectivity of medical devices further heightens cyber threats, requiring strong protection without compromising operational functions. In Indonesia, the high level of cyber threats and data breach incidents demonstrates the importance of strengthening electronic system security, including those belonging to the TNI. The electronic medical records of TNI personnel constitute sensitive data protected by the Electronic Information and Transactions Law (UU ITE), particularly provisions prohibiting unauthorized access, disclosure of confidential information, and manipulation of electronic data. In addition, Law No. 34 of 2004 on the TNI requires military personnel to safeguard military secrets. Violations may result in criminal, disciplinary, and military sanctions. The National Health Defense System aims to integrate military and civilian health resources to address health threats and strengthen national resilience. Its implementation requires adequate synergy, infrastructure, regulations, resources, and funding. This study employs normative legal research. The results show that cyber crimes in military healthcare services include unauthorized access, medical data manipulation, and ransomware attacks. Vulnerabilities include weaknesses in the Hospital Management Information System (SIMRS), limited infrastructure, slow networks, weak passwords, and incomplete medical data, which may affect the accuracy of soldiers' combat readiness profiles. The handling of cyber crimes involving military medical records has specific characteristics under Law No. 34 of 2004 on the TNI, as soldiers' medical records are classified as military secrets. Data breaches may result in criminal, disciplinary, and military judicial sanctions because they have the potential to threaten national security and defense.

Keywords: Cyber Crime, Military Digital Medical Records, TNI Law..

A. Pendahuluan

Transformasi digital dalam kesehatan militer melalui rekam medis elektronik (RME), telemedicine, kecerdasan buatan, dan analitik data meningkatkan efisiensi, akses, serta kualitas pelayanan kesehatan (Bachuk, 2024; Khan, 2018). Namun, digitalisasi juga menimbulkan tantangan berupa privasi, beban pengelolaan data, regulasi, dan keamanan siber. RME rentan terhadap pencurian, manipulasi, ransomware, serta kebocoran data akibat kesalahan manusia, sistem lama, lemahnya investasi keamanan, dan tingginya konektivitas perangkat medis (Budiman et al., 2023; Almohesen et al., 2024). Karena itu, diperlukan enkripsi, blockchain, kecerdasan buatan, autentikasi multifaktor, serta kebijakan keamanan siber yang komprehensif.

Kerentanan tersebut semakin penting dalam sistem kesehatan militer karena perangkat medis yang terhubung dengan jaringan dapat menjadi sasaran serangan siber. Kondisi ini menciptakan dilema antara keamanan sistem dan kebutuhan interoperabilitas serta kelancaran pelayanan kesehatan. Rendahnya pendidikan dan tenaga ahli keamanan siber juga menjadi persoalan, sementara sektor kesehatan merupakan salah satu sektor yang banyak mengalami pelanggaran data (Razaque et al., 2019; Williams & Woodward, 2015).

Di Indonesia, perkembangan keamanan siber menunjukkan kebutuhan akan penguatan ketahanan siber nasional. Tingginya jumlah serangan siber dan kasus kebocoran data menunjukkan bahwa sistem kesehatan, termasuk sistem kesehatan militer, membutuhkan perlindungan yang lebih kuat. TNI memiliki kepentingan strategis untuk mengamankan sistem elektronik dan jaringan informasi sekaligus mendukung keamanan siber nasional (Munawarroh et al., 2019).

RME anggota TNI merupakan data sensitif yang mendapat perlindungan hukum. UU ITE melarang akses tanpa hak, manipulasi atau pemalsuan data, serta pengungkapan informasi elektronik rahasia. Dengan demikian, peretasan, perubahan, dan penyebaran RME prajurit tanpa izin dapat menimbulkan konsekuensi pidana. Selain itu, kewajiban menjaga rahasia juga ditegaskan dalam UU No. 34 Tahun 2004 tentang TNI dan diperkuat melalui ketentuan hukum disiplin militer.

Dalam perspektif yang lebih luas, Sistem Pertahanan Kesehatan Nasional merupakan upaya mengintegrasikan sumber daya kesehatan militer dan sipil untuk menghadapi ancaman

kesehatan serta mendukung ketahanan nasional. Penguatan sistem tersebut membutuhkan integrasi, perencanaan strategis, infrastruktur, regulasi, dan sinergi antara Sistem Kesehatan Nasional dan Sistem Kesehatan Pertahanan (Lardo, 2020; Winarno et al., 2021). Implementasinya masih menghadapi tantangan berupa alokasi sumber daya, kesiapan infrastruktur, pembiayaan, dan keberlanjutan program Jaminan Kesehatan Nasional (Briando et al., 2021; Azizah et al., 2024).

B. Metodologi

Penelitian ini merupakan penelitian studi kepustakaan, yang menelaah bagaimana analisis hukum terhadap cyber crime pada rekam medis militer dengan menggunakan pendekatan studi pada UU TNI. Pendekatan ini digunakan untuk menganalisis peran dari UU tersebut dalam penanganan kejahatan cyber terutama pada rekam medis militer. Penelitian ini dilakukan melalui pengkajian terhadap berbagai peraturan perundang-undangan yang terkait dengan analisis hukum terhadap cyber crime pada rekam medis militer. Oleh karena itu, objek kaitannya tentang teori-teori hukum, asas-asas hukum, sistematika hukum, taraf sinkronisasi hukum, perbandingan dan Sejarah,serta norma hukum yang berlaku. Penelitian hukum ini disebut sebagai penelitian hukum normative (Doctrinal Legal Research) yang djelaskan oleh Soerjono Soekanto dan Sri Mamuji sebagai penelitian hukum kepustakaan yaitu penelitian hukum yang dilakukan debgan cara meneliti data Pustaka atau data sekunder. Data Pustaka sebagai data hukum primer dalam penelitian hukum normative adalah meliputi norma-norma atau kaidah dasar hukum yang meliputi undang-undang.

C. Hasil dan Pembahasan

Transformasi digital kesehatan militer melalui RME meningkatkan efisiensi dan kualitas layanan, tetapi juga menimbulkan risiko keamanan siber, seperti kebocoran, manipulasi, dan akses ilegal terhadap data medis. Temuan di beberapa rumah sakit TNI menunjukkan masih adanya keterbatasan infrastruktur, pemahaman SDM, pengelolaan anggaran, serta keamanan akses yang dapat membuka celah siber.

Kebocoran data e-HAC dan BPJS pada 2021 menunjukkan bahwa data kesehatan memiliki nilai strategis dan dapat berdampak pada keamanan nasional, terutama karena terdapat data prajurit TNI dalam sistem BPJS. Dalam konteks militer, RME mengandung informasi tentang kondisi dan kesiapan prajurit sehingga perlu diperlakukan sebagai informasi yang sangat rahasia. Pelanggaran dapat menimbulkan konsekuensi pidana maupun sanksi hukum militer.

Karena itu, perlindungan RME militer memerlukan penguatan regulasi, keamanan teknologi, peningkatan kompetensi SDM, serta sinergi TNI, Kemhan, BSSN, dan Polri. Penguatan tersebut penting untuk menjamin kerahasiaan, integritas, dan ketersediaan data sekaligus menjaga kedaulatan digital dan pertahanan nasional.

D. Kesimpulan

Berdasarkan hasil penelitian Bentuk kejahatan siber (cyber crime) pada layanan kesehatan militer mencakup akses ilegal (hacking), manipulasi data medis, dan ancaman ransomware. Investigasi di berbagai rumah sakit TNI menunjukkan adanya kerentanan hibrida: secara teknis ditemukan fitur Sistem Informasi Manajemen Rumah Sakit (SIMRS) yang belum optimal, kendala infrastruktur seperti keterbatasan komputer dan jaringan yang lambat, serta penggunaan kata sandi yang lemah. Secara administratif, ditemukan risiko manipulasi pasif berupa ketidaklengkapan pengisian data (seperti pengisian diagnosa hanya dengan tanda "-") yang berpotensi mengaburkan akurasi profil Combat Readiness (kesiapan tempur) prajurit. Kasus kebocoran data e-HAC dan BPJS Kesehatan menjadi bukti nyata bahwa data medis adalah aset strategis yang jika dikuasai pihak asing, dapat menjadi instrumen spionase untuk memetakan kerentanan nasional. Terdapat konvergensi hukum pada UU TNI No. 34 Tahun 2004 dalam menangani kejahatan siber rekam medis militer. Dimana UU TNI memberikan kekhususan di mana rekam medis militer diklasifikasikan sebagai "Rahasia Tentara". Konsekuensinya, personel militer atau tenaga medis yang membocorkan data tersebut tidak hanya menghadapi sanksi pidana umum, tetapi juga tuntutan disiplin dan peradilan militer karena dianggap mengkhianati Sumpah Prajurit dan membahayakan kedaulatan pertahanan negara.

E. Referensi

Bachuk, O. (2024). DIGITAL TRANSFORMATION IN THE HEALTH CARE SYSTEM. Odesa National University Herald. Economy.

Saad Khan, Military Health System Transformation Implications on Health Information Technology Modernization, Military Medicine, Volume 183, Issue 3-4, March-April 2018, Pages 56–59, https://doi.org/10.1093/milmed/usx100

Limna, P. (2023). The Digital Transformation of Healthcare in The Digital Economy: A Systematic Review . International Journal of Advanced Health Science and Technology, 3(2), 127–132. https://doi.org/10.35882/ijahst.v3i2.244

Erhahiemen P, O'Donnell CA, Gallacher K and Nicholl BI. A systematic review of the experience of treatment burden of digital health for military personnel in primary healthcare. [version 1; peer review: 2 approved]. Health Open Res 2024, 6:9 (https://doi.org/10.12688/healthopenres.13599.1)

Smith DJ, Bono RC, Slinger BJ. Transforming the Military Health System. JAMA. 2017;318(24):2427–2428. doi:10.1001/jama.2017.16718

Lai, E.F., & Friedl, K.E. (2009). Digital soldiers: Transforming personalized health in challenging and changing environments. Proceedings of the 6th International Workshop on Wearable, Micro, and Nano Technologies for Personalized Health, 5-8

Cavoski, S., Vujovic, V., Devrnja, V., Ferenc, B., & Lukić, F. (2022). Digital Transformation in Healthcare Healthcare on Demand. 2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH), 1-6.

Budiman, Mantoro, T., Ratmono, B.M., & Persadha, P.D. (2023). Preventing Cyber Crime in Electronic Medical Records Using Encryption Data. 2023 International Conference on Technology, Engineering, and Computing Applications (ICTECA), 1-6.

Luna, R.D., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C.S. (2016). Cyber threats to health information systems: A systematic review. Technology and Health Care, 24, 1 - 9.

Almohesen, S.A., alnoweser, A.A., al- Nasser, N.S., Bawardi, S.A., & ALFwzan, I.S. (2024). Enhancing the Security of Medical Records in the Age of Cyber Threats: A Comprehensive Approach. Saudi Journal of Medicine.

Razaque, A., Amsaad, F.H., Jaro Khan, M., Hariri, S., Chen, S., Chen, S., & Ji, X. (2019). Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain. IEEE Access, 7, 168774-168797

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical devices (Auckland, N.Z.), 8, 305–316. https://doi.org/10.2147/MDER.S50048

Munawarroh, F., Widodo, P., & Azhary, Y. (2019). Efforts to Strengthen Cyber Defense and Cyber Security of the Indonesian Government in Maintaining National Securityse, JETISH: Jurnal Pendidikan Teknologi Informasi Ilmu Sosial dan Kesehatan E-ISSN: 2964-2507 P-ISSN: 2964-819X Vol. 2 No. 1 March 2023

Putra, A. K. (2014). Harmonisasi Konvensi Cyber Crime dalam Hukum Nasional. Jurnal Ilmu Hukum

Mulawardhana, R. A., & Lisanawati, G. (2020). Tindak Pidana Terkait Akses Akun Mobile Banking dengan Mengaktifkan Kembali Simcard yang Sudah Tidak Aktif. Jurnal Yustika, 23(2)

Lelyana (2022). DENTISTS' ROLE IN STRENGTHENING THE NATIONAL DEFENSE SYSTEM. Jurnal Pertahanan Vol. 8 No. 2 pp. 246-252 DOI: http://dx.doi.org/10.33172/j p.v8i2.1754

Lardo, S. (2019). Indonesia's defense health perspective. Jurnal Pertahanan, 5(1), 46–60. https://doi.org/10.33172/jp.v5i1.425

Winarno, S., Wandawa, G., & Sitam, S. (2021). Analisis implementasi kebijakan Sistem Kesehatan Pertahanan Negara (Siskeshanneg) menghadapi ancaman faktual pandemi COVID-19 di Lembaga Kedokteran Gigi (Ladokgi) Raden Eddy Martadinata. Padjadjaran Journal of Dental Researchers and Students, 5(2), 146–156. https://doi.org/10.24198/pjdrs.v5i2.33356

Mardhani, D. (2020). Security and defence dalam studi ketahanan nasional guna mewujudkan sistem keamanan nasional. Jurnal Pertahanan & Bela Negara, 10(3), 279–298. https://doi.org/10.33172/jpbh.v10i3.862

Primasari, K.L. (2015). Analisis Sistem Rujukan Jaminan Kesehatan Nasional RSUD. Dr. Adjidarmo Kabupaten Lebak. Jurnal Administrasi Rumah Sakit Indonesia.

Azizah, S.N., Septiana, W., & Wasir, R. (2024). Membangun Sistem Jaminan Kesehatan Nasional yang Berkualitas: Kajian Literatur untuk Mempelajari Tantangan dan Merumuskan Solusi. An-Najat.

Salim, D. L. F. (2020). Aksesibilitas pembiayaan kesehatan dalam program Jaminan Kesehatan Nasional. Lex et Societatis, 8(4), 104–114. https://doi.org/10.35796/les.v8i4.30915

Al-Khater, W., Al-Maadeed, S., Ahmed, A., Sadiq, A., & Khan, M. (2020). Comprehensive Review of Cybercrime Detection Techniques. IEEE Access, 8, 137293-137311. https://doi.org/10.1109/access.2020.3011259.

Thomas, A. (2023). Analysis on Cyber Crimes and Preventive Measures. International Journal for Research in Applied Science and Engineering Technology. https://doi.org/10.22214/ijraset.2023.52481.

Pandey, P., & Kapoor, A. (2025). Cybercrime in the digital era: Impacts, awareness, and strategic solutions for a secure future. Sachetas, 4(1), 32–37. https://doi.org/10.55955/410004

Ho, H., Ko, R., & Mazerolle, L. (2022). Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. Comput. Secur., 115, 102611. https://doi.org/10.1016/j.cose.2022.102611.

Chatterjee, S., Kar, A., Dwivedi, Y., & Kizgin, H. (2019). Prevention of cybercrimes in smart cities of India: from a citizen's perspective. Inf. Technol. People, 32, 1153-1183. https://doi.org/10.1108/itp-05-2018-0251.

Phillips, K., Davidson, J., Farr, R., Burkhardt, C., Caneppele, S., & Aiken, M. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences. https://doi.org/10.3390/forensicsci2020028.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1-10

Ponemon Institute. (2020). Cost of a Data Breach Report 2020. Dapat diakses di: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

He, Y., Aliyu, A., Evans, M., & Luo, C. (2020). Health care cybersecurity challenges and solutions under the climate of COVID-19: A scoping review. Journal of Medical Internet Research, 23(4), e21747. Dapat diakses di: https://www.jmir.org/2020/4/e21747/

Williams, M., & Shah, A. (2019). Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward. Maturitas, 131, 1-7. Dapat diakses di: https://www.maturitas.org/article/S0378-5122(19)30880-9/fulltext

WONG, Mary W. S.. Cyber-trespass and 'unauthorized access' as legal mechanisms of access control: Lessons from the US experience. (2007). International Journal of Law and Information Technology. 15, (1), 90-128. Available at: https://ink.library.smu.edu.sg/sol_research/2820

Kane, S. (2020). Available, Granted, Revoked: A New Framework for Assessing Unauthorized Access Under the Computer Fraud and Abuse Act. University of Chicago Law Review, 87, 5.

Kartika, R.N. (2018). EFEKTIVITAS UNSUR “MANIPULASI” INFORMASI ELEKTRONIK SEOLAH-OLAH DATA OTENTIK MENURUT PASAL 35 UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK (STUDI DI POLRES KABUPATEN MALANG DAN DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN MALANG).

Malii, B. (2025). Civil law regime of protection of the right to medical secrecy. Theory and Practice of Intellectual Property.

Anwar, T. M., Tambun, J. G., & Jaeni, A. (2025). Juridical analysis of the misuse of electronic medical records in the perspective of the electronic information and transaction law. Pranata Hukum, 20(1), 26–36. https://doi.org/10.36448/pranatahukum.v20i1.380

Sá-Correia, L., Cruz-Correia, R.J., & Rodrigues, P.P. (2019). Illegitimate HIS access by healthcare professionals: scenarios, use cases and audit trail-based detection model. CENTERIS/ProjMAN/HCist

Tombolotutu, R.N., Chandra, T.Y., & Mau, H.A. (2024). Proving Illegal Access in Combating Cybercrime in Indonesia. Journal of Law and Regulation Governance.

Mulawardhana, R.A., & Lisanawati, G. (2020). Tindak Pidana Terkait Akses Akun Mobile Banking dengan Mengaktifkan Kembali Simcard yang Sudah Tidak Aktif. JURNAL YUSTIKA: MEDIA HUKUM DAN KEADILAN.

Susanto, E., Rahman, H., Nurazizah, N., Aisyah, L., & Puspitasari, E. (2021). Politik hukum pidana dalam penegakkan Undang-Undang Informasi dan Transaksi Elektronik (ITE). Journal Kompilasi Hukum, 6(2). https://doi.org/10.29303/jkh.v6i2.76Kusuma, R., & Sembiring, F.(2022). Mapping legal professionals and layfolk on freedom of speech according to constitution, the electronic information and transaction law. International Journal of

Research in Business and Social Science (2147- 4478), 11(1).
Afisa, A., Qodir, Z., Habibullah, A., & Sugiharto, U. (2024). Analysis of the ITE Law on Digital Rights and Democratic Values in Indonesia. The Journal of Society and Media.
Bretag, T., et al. (2019). Research integrity and misconduct: A systematic review of the literature. Studies in Higher Education, 44(8), 1433-1452. https://doi.org/10.1080/03075079.2018.1455058
Fanelli, D. (2018). How many scientists fabricate and falsify research? A systematic review and meta-analysis of survey data. PLOS ONE, 4(5), e5738. https://doi.org/10.1371/journal.pone.0005738
Wicherts, J. M., et al. (2022). The importance of transparency in data analysis. Nature Human Behaviour, 6(3), 321-330. https://doi.org/10.1038/s41562-022-01333-7
Simmons, J. P., et al. (2021). False-positive psychology: Undisclosed flexibility in data collection and analysis allows presenting anything as significant. Psychological Science, 22(11), 1359-1366. https://doi.org/10.1177/0956797611417632
Alshaikh, H., Ramadan, N., & Ahmed, H. (2020). Ransomware Prevention and Mitigation Techniques. International Journal of Computer Applications. https://doi.org/10.5120/ijca2020919899.
Monika, N.F., Universitas, L., Malikussaleh, Firdaus, R., & Malikussaleh, U. (2024). Analisis Bahaya Serangan Ransomeware Terhadap Layanan Perbankan. Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika.
Kholis, I.M. (2025). Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia. Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam.
Nyonyoh, R. (2025). Ransomware and the Vulnerability of Critical Infrastructure: A National Security and Economic Analysis. Asian Journal of Economics, Business and Accounting. https://doi.org/10.9734/ajeba/2025/v25i41759.
Malik, V., Khanna, A., Sharma, N., & Nalluri, S. (2024). Trends in Ransomware Attacks: Analysis and Future Predictions. International Journal of Global Innovations and Solutions (IJGIS). https://doi.org/10.21428/e90189c8.f2996624.
Venkatesh, G., Anne, W., & Sridevi, U. (2024). A recent review of ransomware attacks on healthcare industries. Int. J. Syst. Assur. Eng. Manag., 15, 5078-5096. https://doi.org/10.1007/s13198-024-02496-4.
Avery, A., Baker, E., Wright, B., Avery, I., & Gomez, D. (2024). Media Framing and Portrayals of Ransomware Impacts on Informatics, Employees, and Patients: Systematic Media Literature Review. Journal of Medical Internet Research, 27. https://doi.org/10.2196/59231.
Temara, S. (2024). The Ransomware Epidemic: Recent Cybersecurity Incidents Demystified. Asian Journal of Advanced Research and Reports. https://doi.org/10.9734/ajarr/2024/v18i3610.
Anbiyaa, F. (2025). Model Pemolisian Siber: Pendekatan Community Policing Dan E-Policing Dalam Penanggulangan Kejahatan Ransomware. Cerdika: Jurnal Ilmiah Indonesia.
Tully, J., Gabriel, R., Waterman, R., & Dameff, C. (2025). Digital Disasters: The Growing Threat of Healthcare Ransomware.. Anesthesiology, 142 6, 1005-1008 . https://doi.org/10.1097/ALN.0000000000005442.
McGlave, C., Neprash, H., & Nikpay, S. (2023). Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4579292.
Genevieve P.Kanter, P., Jack Kufahl, B., & I.Glenn Cohen, J. (2021). Beyond Security Patches-Fundamental Incentive Problems in Health Care Cybersecurity.. JAMA health forum, 2 10, e212969 . https://doi.org/10.1001/jamahealthforum.2021.2969.
Neprash, H., McGlave, C., Cross, D., Virnig, B., Puskarich, M., Huling, J., Rozenshtein, A., & Nikpay, S. (2022). Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. JAMA Health Forum, 3. https://doi.org/10.1001/jamahealthforum.2022.4873.
Reddy, J., Elsayed, N., ElSayed, Z., & Ozer, M. (2023). A Review on Data Breaches in Healthcare Security Systems. International Journal of Computer Applications. https://doi.org/10.5120/ijca2023922333.
Cornejo, G., Lee, J., & Russell, B. (2024). A thematic analysis of ransomware incidents among United States hospitals, 2016–2022. Health and Technology. https://doi.org/10.1007/s12553-024-00890-3.
Novita, A., Fatmanegara, F., Runtuwene, F., Samuela, J., & Syahbani, M. (2023). CYBER SECURITY

THREATS; ANALISIS DAN MITIGASI RESIKO RANSOMWARE DI INDONESIA. Jurnal Ilmiah Sistem Informasi. https://doi.org/10.46306/sm.v3i1.91.

Temara, S. (2024). The Ransomware Epidemic: Recent Cybersecurity Incidents Demystified. Asian Journal of Advanced Research and Reports. https://doi.org/10.9734/ajarr/2024/v18i3610.

Nagar, G. (2024). The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies. International Journal of Scientific Research and Management (IJSRM). https://doi.org/10.18535/ijsrm/v12i06.ec09.

Olasunkanmi, O. (2025). Ransomware trends and mitigation strategies: A comprehensive review. Global Journal of Engineering and Technology Advances. https://doi.org/10.30574/gjeta.2025.22.3.0038.

Ariyaningsih, S., Andrianto, A.A., Kusuma, A.S., & Prastyanti, R.A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. Justisia: Jurnal Ilmu Hukum.

Br.Sembiring, T., & Meutia, C.Y. (2024). Analysis of the Use of Electronic Medical Records Regarding Law Number 17 of 2023 in Indonesia. Formosa Journal of Science and Technology.

Nurrahma, A. N., Larasati, T. A., Kurniati, I., & Pramesona, B. A. (2023). Electronic medical records in primary health care facilities. Review of Primary Care Practice and Education, 6(2), 60–64. https://doi.org/10.22146/rpcpe.79085

Putri, Y. W., Saragih, T. R., & Purba, S. H. (2024). Implementasi dan dampak penggunaan sistem rekam medis elektronik (RME) pada pelayanan kesehatan. Sehat Rakyat: Jurnal Kesehatan Masyarakat, 3(4), 255–264. https://doi.org/10.54259/sehatrakyat.v3i4.3449

Warianti, S., & Sutabri, T. (2024). Analis pengukuran kualitas pengelolaan rekam medis elektronik menggunakan metode Delone and McLean pada RSUD Dr. H. Mohamad Rabain. Uranus: Jurnal Ilmiah Teknik Elektro, Sains dan Informatika, 2(4), 192–204. https://doi.org/10.61132/uranus.v2i4.499

Benson, T., & Grieve, G. (2016). Principles of Health Interoperability: SNOMED CT, HL7 and FHIR. Principles of Health Interoperability.

Rezaeibagha, F., Win, K.T., & Susilo, W. (2015). A Systematic Literature Review on Security and Privacy of Electronic Health Record Systems: Technical Perspectives. Health Information Management Journal, 44, 23 - 38.

Kiwanuka, A., Amiyo, M., Nabukenya, J., et al. (2023). Constraints to and enablers for contextualizing digital health terminology standards in Uganda's health services: A qualitative case study. Oxford Open Digital Health, 1, oqad003. https://doi.org/10.1093/oodh/oqad003

Budiyanti, R. T., Herlambang, P. M., Fuad, A., & Kusumastuti, W. (2023). Integration of electronic medical record and SATUSEHAT's platform: Patient's legal protection perspective. International Journal of Health Literacy and Science, 1(2), 1–8. https://doi.org/10.60074/ihelis.v1i2.18

Mayasafira, S. D., & Almansoob, M. (2024). ELECTRONIC MEDICAL RECORDS AS DIGITAL TRANSFORMATION IN INDONESIAN HEALTH SERVICES 4.0. INTERNATIONAL JOURNAL OF NURSING AND MIDWIFERY SCIENCE (IJNMS), 8(2), 229-239. https://doi.org/10.29082/IJNMS/2024/Vol8/Iss2/609

Muñoz, Pilar, Trigo, Jesús D., Martínez, Ignacio, Muñoz, Adolfo, Escayola, Javier, García, José, The ISO/EN 13606 Standard for the Interoperable Exchange of Electronic Health Records, Journal of Healthcare Engineering, 2, 316579, 24 pages, 2011. https://doi.org/10.1260/2040-2295.2.1.1

Martíez, I., Escayola, J., Martínez-Espronceda, M., Munoz, P., Trigo, J.D., Muñoz, A., Led, S., Serrano, L., & García, J. (2010). Seamless integration of ISO/IEEE11073 personal health devices and ISO/EN13606 electronic health records into an end-to-end interoperable solution. Telemedicine journal and e-health : the official journal of the American Telemedicine Association, 16 10, 993-1004 .

Bercic, B., & George, C.E. (2008). Compiling Medical Data into National Medical Databases: Legitimate Practice or Data Protection Concern

Welzer, T., Hölbl, M., Druzovec, M., Klopcic, B., Brumen, B., Jaakkola, H., & Bonacic, M. (2009). Medical Personal Data in Secure Information Systems. International United Information Systems Conference.

Wilén, N., & Strömbom, L. (2021). A versatile organisation: Mapping the military's core roles in a changing security environment. European Journal of International Security, 7, 18 - 37. https://doi.org/10.1017/eis.2021.27.

Balsys, P. (2020). Values and identity of contemporary military officer in the context of national security. Challenges to national defence in contemporary geopolitical situation. https://doi.org/10.47459/cndcgs.2020.23.

Hasselbladh, H. (2025). The shadow of war – The making of military institutional specificity. Dialogues in Sociology. https://doi.org/10.1177/29768667251349925.

Ksenofontov, V. (2021). Social role of the military sphere of national security. Proceedings of the National Academy of Sciences of Belarus, Humanitarian Series. https://doi.org/10.29235/2524-2369-2021-66-4-391-401.

Meerveld, H., & Lindelauf, R. (2024). Data Science in Military Decision-Making: Foci and Gaps. Global Society, 39, 103 - 129. https://doi.org/10.1080/13600826.2024.2353657.

Dhillon, N., Jeon, N., Gurkan, U., Gupta, A., Bonomo, R., Drummy, L., Zhang, M., & Chance, M. (2023). Military Medicine and Medical Research as a Source of Inspiration and Innovation to Solve National Security and Health Challenges in the 21st Century. Pathogens and Immunity, 8, 51 - 63. https://doi.org/10.20411/pai.v8i1.596.

Kellermann, A., Kotwal, R., & Rasmussen, T. (2023). Military Medicine's Value to US Health Care and Public Health: Bringing Battlefield Lessons Home.. JAMA network open, 6 9, e2335125 . https://doi.org/10.1001/jamanetworkopen.2023.35125.

De Vries, H., Van Der Wal, S., Delahaij, R., Venrooij, W., & Kamphuis, W. (2025). Real-time monitoring of military health and readiness: a perspective on future research. Frontiers in Digital Health, 7. https://doi.org/10.3389/fdgth.2025.1542140.

Rajput, V., Phursule, R., Kanjalkar, J., Patil, R., Deshpande, A., & Joshi, V. (2025). Soldier Health Monitoring- A Game Changer in Military Technology. Communications on Applied Nonlinear Analysis. https://doi.org/10.52783/cana.v32.3284.

Koehlmoos, T., Korona-Bailey, J., Elzey, J., Marshall, B., & Shanley, L. (2024). Ethical use of big data for healthy communities and a strong nation: unique challenges for the Military Health System. BMC Proceedings, 18. https://doi.org/10.1186/s12919-024-00308-y.

Roković, V., & Ajzenhamer, V. (2020). Political discourse, military and securitization of health nexus: contemporary security challenges and the military role in public health security. , 66, 45-75. https://doi.org/10.22182/spm.6642019.3.

Thomas, B. (2022). Preparing for the Future of Combat Casualty Care: Opportunities to Refine the Military Health System's Alignment with the National Defense Strategy.. Rand health quarterly, 9 3, 18 . https://doi.org/10.7249/rr-a713-1.

Tallowin, S., Naumann, D., & Bowley, D. (2021). Defence Healthcare Engagement: A UK Military Perspective to Improve Healthcare Leadership and Quality of Care Overseas. Journal of Healthcare Leadership, 13, 27 - 34. https://doi.org/10.2147/JHL.S224906.

Bullock, G., Fallowfield, J., De La Motte, S., Arden, N., Fisher, B., Dooley, A., Forrest, N., Fraser, J., Gourlay, A., Hando, B., Harrison, K., Hayhurst, D., Molloy, J., Newman, P., Robitaille, E., Teyhen, D., Tiede, J., Williams, E., Williams, S., Van Tiggelen, D., VanWyngaarden, J., Westrick, R., Emery, C., Collins, G., & Rhon, D. (2025). Minimal Data Elements for Surveillance and Reporting Of Musculoskeletal Injuries in the MILitary (ROMMIL) International Consensus Statement.. Medicine and science in sports and exercise. https://doi.org/10.1249/MSS.0000000000003737.

Juman, L., Schneider, E., Clifton, D., & Koehlmoos, T. (2024). Common Data Elements and Databases Essential for the Study of Musculoskeletal Injuries in Military Personnel.. Military medicine. https://doi.org/10.1093/milmed/usae241.

Torab-Miandoab, A., Basiri, M., Dabbagh-Moghaddam, A., & Gholamhosseini, L. (2025). Electronic health record in military healthcare systems: A systematic review. PLOS ONE, 20. https://doi.org/10.1371/journal.pone.0313641.

Amin, M., Setyonugroho, W., & Hidayah, N. (2021). Implementasi Rekam Medis Elektronik: Sebuah Studi Kualitatif. JATISI (Jurnal Teknik Informatika dan Sistem Informasi), 8(1), 430–442. https://doi.org/10.35957/jatisi.v8i1.557

Apriliyani, S. (2021). Penggunaan Rekam Medis Elektronik Guna Menunjang Efektivitas Pendaftaran Pasien Rawat Jalan di Klinik Dr. Ranny. Cerdika: Jurnal Ilmiah Indonesia, 1(10), 1399–1410