UNIVERSITAS
GADJAH MADA
Analisis Komparatif Keamanan Pertukaran Payload Rekam Medis Elektronik Berbasis HL7 FHIR pada Pendekatan SATUSEHAT, AES-GCM 128-Bit dengan ECC, dan CHACHA20-POLY1305
Febriano Ahdan Nadif, Dr. Nur Rokhman, S.Si., M.Kom.; Muhammad Oriza Nurfajri, S.Kom., M.IT.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR PUSTAKA

Abunadi, I. and Kumar, R. (2021) 'BSF-EHR: Blockchain Security Framework for Electronic Health Records of Patients', *Sensors*, 21(8), p. 2865. Available at: https://doi.org/10.3390/s21082865.

Abirami, D. N. and Anbarasi, M. S. (2024) 'An Efficient Hybrid Elliptic Curve Cryptography for Securing E-Healthcare Data in Cloud Environment', International Journal of Electronics and Communication Engineering, 11(12), pp. 189–205. Available at: https://doi.org/10.14445/23488549/IJECE-V11I12P118.

Acheampong, R. *et al.* (2025) 'Enhancing Security and Authenticity in Immersive Environments', *Information (Switzerland)*, 16(3), pp. 1–23. Available at: https://doi.org/10.3390/info16030191.

Andrianto, W.S.H. (2022) 'Catatan Sederhana untuk Permenkes No. 24 Tahun 2022 tentang Rekam Medis'. FH-UI. Available at: https://law.ui.ac.id/catatan-sederhana-untuk-permenkes-no-24-tahun-2022-tentang-rekam-medis-oleh-wahyu-andrianto-s-h-m-h/.

Aqeel, S. *et al.* (2025) 'Enhancing IoT security with a DNA-based lightweight cryptography system', *Scientific Reports*, 15(1), p. 13367. Available at: https://doi.org/10.1038/s41598-025-96292-0.

Arizal, A., Sidabutar, J. and Yulianti, N. (2022) *Kriptografi: Teknik Keamanan Data*.

Arrasily, N.F. *et al.* (2025) 'Optimalisasi Pengelolaan Data Pasien Melalui Integrasi Sistem Informasi Rumah Sakit Berbasis Digital', *Journal of Innovative and Creativity*, 5(2), pp. 13888–13910. Available at: https://doi.org/10.31004/joecy.v5i2.2243.

Python Cryptographic Authority (2024) 'cryptography Library Documentation'. Available at: https://cryptography.io/.

Ayaz, M. *et al.* (2021) 'Correction: The Fast Health Interoperability Resources (FHIR) Standard: Systematic Literature Review of Implementations, Applications, Challenges and Opportunities', *JMIR Medical Informatics*, 9(8), p. e32869. Available at: https://doi.org/10.2196/32869.

Chenthara, S. *et al.* (2019) 'Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing', *IEEE Access*, 7, pp. 74361–74382. Available at: https://doi.org/10.1109/ACCESS.2019.2919982.

Chart.js Contributors (2024) 'Chart.js: Simple yet flexible JavaScript charting library (Release 4.4.x)'. Available at: https://www.chartjs.org/.

Danmadiyah, S. (2020) 'Daftar Data Sensitif dalam RUU Pelindungan Data Pribadi Perlu Disempurnakan'. ELSAM. Available at: https://www.elsam.or.id/teknologi-dan-ham/daftar-data-sensitif-dalam-ruu-pelindungan-data-pribadi-perlu-disempurnakan.

Bahri, D.S. and Fauzan, M.A.R. (2025) 'IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) UNTUK MENINGKATKAN KEAMANAN PASSWORD PADA APLIKASI TO-DO LIST BERBASIS ANDROID DENGAN METODE AGILE', *Informatika: Jurnal Teknik Informatika dan Multimedia*, 5(2), pp. 164–171.

UNIVERSITAS
GADJAH MADA
Analisis Komparatif Keamanan Pertukaran Payload Rekam Medis Elektronik Berbasis HL7 FHIR pada Pendekatan SATUSEHAT, AES-GCM 128-Bit dengan ECC, dan CHACHA20-POLY1305
Febriano Ahdan Nadif, Dr. Nur Rokhman, S.Si., M.Kom.; Muhammad Oriza Nurfajri, S.Kom., M.IT.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

Available at: https://doi.org/10.51903/informatika.v5i2.1367.

Degabriele, J.P. *et al.* (2021) 'The Security of ChaCha20-Poly1305 in the Multi-User Setting', *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21)*, pp. 1981–2003. Available at: https://doi.org/10.1145/3460120.3484814.

Dworkin, M. (2007) *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-38D.

Faisal, H.P. and 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, pp. e59651–e59651. Available at: https://doi.org/10.2196/59651.

Fernández-Alemán, J.L. *et al.* (2013) 'Security and privacy in electronic health records: A systematic literature review', *Journal of Biomedical Informatics*, 46(3), pp. 541–562. Available at: https://doi.org/10.1016/j.jbi.2012.12.003.

Filkins, B.L. et al. (2016) 'Privacy and security in the era of digital health: what should translational researchers know and do about it?', *American journal of translational research*, 8(3), p. 1560.

Finliana, S.C. *et al.* (2025) 'Review of the Security and Confidentiality of Electronic Medical Records At Uptd Puskesmas Kedawung in 2025', *Jurnal Kesehatan, Sains, Dan Teknologi (Jakasakti)*, 4(2), pp. 460–469. Available at: https://doi.org/10.36002/js.v4i2.3860.

Reddy, G.J. and Devi, T.U. (2025) 'Algorithms for Enhanced Security and Data Sharing in Blockchain-Driven Healthcare Systems', *International Journal of Computational and Experimental Science and Engineering*, 11(2). Available at: https://doi.org/10.22399/ijcesen.1162.

Ghani, N.A. *et al.* (2025) 'Edge-Enabled Hybrid Encryption Framework for Secure Health Information Exchange in IoT-Based Smart Healthcare Systems', *Sensors*, 25(24), p. 7583. Available at: https://doi.org/10.3390/s25247583.

Gour, A. *et al.* (2024) 'Hybrid Cryptographic Approach: For Secure Data Communication using Block Cipher Techniques', *E3S Web of Conferences*. Edited by P.K. Prabhakar, 556, p. 01048. Available at: https://doi.org/10.1051/e3sconf/202455601048.

Harahap, A.H.H. *et al.* (2023) 'Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder', *Jurnal Manajemen dan Pemasaran Digital*, 1(2), pp. 73–83. Available at: https://doi.org/10.38035/jmpd.v1i2.34.

Hardt, D. (2012) *The OAuth 2.0 Authorization Framework*. Edited by D. Hardt. Internet Engineering Task Force. Available at: https://doi.org/10.17487/rfc6749.

Heryawan, L. *et al.* (2025) 'Fast Healthcare Interoperability Resources (FHIR)–Based Interoperability Design in Indonesia: Content Analysis of Developer Hub's Social Networking Service', *JMIR Formative Research*, 9, pp. e51270–e51270. Available at: https://doi.org/10.2196/51270.

UNIVERSITAS
GADJAH MADA
Analisis Komparatif Keamanan Pertukaran Payload Rekam Medis Elektronik Berbasis HL7 FHIR pada Pendekatan SATUSEHAT, AES-GCM 128-Bit dengan ECC, dan CHACHA20-POLY1305
Febriano Ahdan Nadif, Dr. Nur Rokhman, S.Si., M.Kom.; Muhammad Oriza Nurfajri, S.Kom., M.IT.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

Kementerian Kesehatan Republik Indonesia (2025) 'SATUSEHAT Platform Documentation'. Pusat Data dan Teknologi Informasi - Digital Transformation Office. Available at: https://satusehat.kemkes.go.id/platform/docs/.

Jaya, A.A.G.P.S. et al. (2026) 'Penyelenggaraan rekam medis elektronik oleh fasilitas pelayanan kesehatan: kajian terhadap pelindungan data pribadi pasien', *Prosiding Seminar Nasional Hukum, Bisnis, Sains dan Teknologi*, pp. 67–75. Available at: https://ojs.udb.ac.id/HUBISINTEK/article/view/5848.

Jrejeki (2025) 'Cara Mudah Integrasi RME ke SATUSEHAT untuk Puskesmas'. Available at: https://jrejeki.co.id/site/data?slug=integrasi-rme-satusehat.

Khusna, P.N. (2025) 'Penerapan HL7-FHIR: Potret Komparatif Indonesia dan Best Practice Internasional Menuju Ekosistem Kesehatan Terintegrasi Adopting HL7-FHIR: Indonesia's Journey and Global Best Practices for Healthcare Interoperability', (June), p. 7. Available at: https://www.researchgate.net/publication/392521960_Penerapan_HL7-FHIR_Potret_Komparatif_Indonesia_dan_Best_Practice_Internasional_Menuju_Ekosistem_Kesehatan_Terintegrasi_Adopting_HL7-FHIR_Indonesia's_Journey_and_Global_Best_Practices_for_Healthcare_In.

Krawczyk, H. and Eronen, P. (2010) *HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*. Internet Engineering Task Force.

Kumar, T. *et al.* (2021) 'A Low Area High Speed FPGA Implementation of AES Architecture for Cryptography Application', *Electronics*, 10(16), p. 2023. Available at: https://doi.org/10.3390/electronics10162023.

Purba, G.C.M. and Id Hadiana, A. (2023) 'Pengamanan Citra Medis Berbasis Steganografi dan Kriptografi Dengan Menggunakan Metode End Of File Dan Advanced Encryption Standard', *Informatics and Digital Expert (INDEX)*, 4(1), pp. 1–9. Available at: https://doi.org/10.36423/index.v4i1.878.

Mandel, J.C. *et al.* (2016) 'SMART on FHIR: a standards-based, interoperable apps platform for electronic health records', *Journal of the American Medical Informatics Association*, 23(5), pp. 899–908. Available at: https://doi.org/10.1093/jamia/ocv189.

Martínez, A.L. *et al.* (2026) 'Breaking barriers in healthcare: A secure identity framework for seamless access', *Computer Standards & Interfaces*, 95, p. 104020. Available at: https://doi.org/10.1016/j.csi.2025.104020.

Maulana, H. *et al.* (2025) 'PERANCANGAN SISTEM KEAMANAN FILE MENGGUNAKAN HYBRID ENCRYPTION UNTUK PERLINDUNGAN DATA', *Jurnal RESTIKOM : Riset Teknik Informatika dan Komputer*, 7(1), pp. 87–96. Available at: https://doi.org/10.52005/restikom.v7i1.420.

McGrew, D. (2025) 'Galois Counter Mode', *Encyclopedia of Cryptography, Security and Privacy*. Cham: Springer Nature Switzerland, pp. 994–997. Available at: https://doi.org/10.1007/978-3-030-71522-9_451.

Meliana, S.E. et al. (2026) *TRANSFORMASI DIGITAL REKAM MEDIK*. Husni

UNIVERSITAS
GADJAH MADA
Analisis Komparatif Keamanan Pertukaran Payload Rekam Medis Elektronik Berbasis HL7 FHIR pada Pendekatan SATUSEHAT, AES-GCM 128-Bit dengan ECC, dan CHACHA20-POLY1305
Febriano Ahdan Nadif, Dr. Nur Rokhman, S.Si., M.Kom.; Muhammad Oriza Nurfajri, S.Kom., M.IT.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

Abdul Muchlis.

Mohamed, Y.A. *et al.* (2026) 'A survey on health spending and comprehensive eGuide for healthcare: Challenges, implementation and future directions', *Sustainable Futures*, 11(November 2025), p. 101584. Available at: https://doi.org/10.1016/j.sftr.2025.101584.

Mukhiya, S.K. and Lamo, Y. (2021) 'An HL7 FHIR and GraphQL approach for interoperability between heterogeneous Electronic Health Record systems', *Health Informatics Journal*, 27(3), p. 14604582211043920. Available at: https://doi.org/10.1177/14604582211043920.

Mariani, N.K. (2025) 'ANALISIS ASPEK KEAMANAN DATA REKAM MEDIS DALAM IMPLEMENTASI REKAM MEDIS ELEKTRONIK DI RUMAH SAKIT UMUM KLUNGKUNG', *MAINTEKKES : The Journal of Management Information and Health Technology*, 3(2), pp. 79–91. Available at: https://doi.org/10.36049/maintekkes.v3i2.420.

Nir, Y. and Langley, A. (2018) *ChaCha20 and Poly1305 for IETF Protocols*. RFC 8439. Internet Engineering Task Force.

NIST (2023) 'NIST Revises the Digital Signature Standard (DSS) and Publishes a Guideline for Elliptic Curve Domain Parameters'. Available at: https://csrc.nist.gov/news/2023/nist-releases-fips-186-5-and-sp-800-186.

Okpu, O.E. *et al.* (2024) 'Comparative Performance Analysis of Cryptographic Techniques for Securing the Physical Layer in Internet of Medical Things (IoMT) Systems', *Int. J. Comput. Sci. Math. Theory*, 10(2), pp. 157–169. Available at: https://doi.org/10.56201/ijcsmt.v10.no2.2024.pg157.169.

Pramesti, D.P.A., Ayuningtyas, D. and Verdi, R. (2024) 'KEAMANAN DAN KERAHASIAAN DATA MEDIS PASIEN DALAM IMPLEMENTASI REKAM MEDIS ELEKTRONIK : TINJAUAN SISTEMATIS', *PREPOTIF : JURNAL KESEHATAN MASYARAKAT*, 8(3), pp. 7691–7702. Available at: https://doi.org/10.31004/prepotif.v8i3.38445.

Pratama, R.R., Virgian, D. and Sakti, S.Y. (2025) 'IMPLEMENTASI HYBRID ENCRYPTION ECC-AES UNTUK PENGAMANAN KOMUNIKASI DAN BERBAGI FILE BERBASIS WEB', *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, pp. 104–113. Available at: https://senafti.budiluhur.ac.id/senafti/article/view/1773.

Pallets Projects (2024) 'Flask Documentation (Release 3.0.x)'. Available at: https://flask.palletsprojects.com/.

Purba, L.C. *et al.* (2019) 'PENGAMANAN DATA PADA LALU LINTAS DATA MENGGUNAKAN FUNGSI KRIPTOGRAFI RSA DARI SERANGAN SNOOPING', *TECHSI - Jurnal Teknik Informatika*, 11(3), pp. 419–430. Available at: https://doi.org/10.29103/techsi.v11i3.1971.

Purnamasari, D.N., Sudarsono, A. and Kristalina, P. (2019) 'Secure e-Health Record System Using Identity-based Encryption with Embedded Key', *International Journal on Advanced Science, Engineering and Information Technology*, 9(5), pp. 1496–1504. Available at: https://doi.org/10.18517/ijaseit.9.5.8278.

Rani, D.M. and Widyaningrum, B.N. (2025) 'Evaluasi Keamanan Informasi Sistem Rekam Medis Elektronik di RSI Sultan Agung', *Jurnal Manajemen*

UNIVERSITAS
GADJAH MADA
Analisis Komparatif Keamanan Pertukaran Payload Rekam Medis Elektronik Berbasis HL7 FHIR pada Pendekatan SATUSEHAT, AES-GCM 128-Bit dengan ECC, dan CHACHA20-POLY1305
Febriano Ahdan Nadif, Dr. Nur Rokhman, S.Si., M.Kom.; Muhammad Oriza Nurfajri, S.Kom., M.IT.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

Informasi Kesehatan (Health Information Management), 10(1), pp. 52–62. Available at: https://ojs.stikessaptabakti.ac.id/jmis/article/view/636.

Saarinen, M.-J. (2011) 'GCM, GHASH and Weak Keys.', *IACR Cryptology ePrint Archive*, 2011, p. 202.

Šafran, V. *et al.* (2025) 'A Scalable and Secured HL7 FHIR Healthcare Platform: Architecture, Load Testing, and Preliminary Findings', *International Journal of Education and Information Technologies*, 19, pp. 128–137. Available at: https://doi.org/10.46300/9109.2025.19.13.

Selvi, P. and Sakthivel, S. (2025) 'A hybrid ECC-AES encryption framework for secure and efficient cloud-based data protection', *Scientific Reports*, 15(1), p. 30867. Available at: https://doi.org/10.1038/s41598-025-01315-5.

Maathavan, K.S.K. and Venkatraman, S. (2022) 'A Secure Encrypted Classified Electronic Healthcare Data for Public Cloud Environment', *Intelligent Automation & Soft Computing*, 32(2), pp. 765–779. Available at: https://doi.org/10.32604/iasc.2022.022276.

Siregar, R.A. (2024) 'Penerapan Permenkes Nomor 24 Tahun 2022 Tentang Rekam Medis Terhadap Efektivitas Pelayanan Kesehatan', *JIHK*, 5(2). Available at: https://doi.org/10.46924/jihk.v5i2.182.

Siregar, R.A. and Sinaga, H.S.R. (2025) 'Aspek hukum perlindungan data pasien dalam penyelenggaraan rekam medis elektronik di Indonesia', *Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat*, 11(1), pp. 106–116.

Sreejith, R. and Senthil, S. (2023) 'Smart Contract Authentication assisted GraphMap-Based HL7 FHIR architecture for interoperable e-healthcare system', *Heliyon*, 9(4), p. e15180. Available at: https://doi.org/10.1016/j.heliyon.2023.e15180.

Sulaksono, D.H. *et al.* (2021) 'Implementasi Kriptografi dengan Metode Elliptic Curve Cryptography (ECC) untuk Aplikasi Chatting Berbasis Android', *Prosiding Seminar Nasional Sains dan Teknologi Terapan*, pp. 570–576.

Suryani, S., Warongan, V.A. and Ayuningtia, A.D. (2025) 'Analisis Penerapan Sistem Rekam Medis Elektronik di Rumah Sakit Mitra Sejati Kota Medan', *JURNAL RISET RUMPUN ILMU KEDOKTERAN*, 4, pp. 330–341. Available at: https://doi.org/10.55606/jurrike.v4i2.6293.

Susanti, A. *et al.* (2024) 'Perbandingan Kinerja dan Keamanan Algoritma Kriptografi Modern AES-GCM dengan CHACHA20-POLY1305', *Infomatek*, 26(2), pp. 253–264. Available at: https://doi.org/10.23969/infomatek.v26i2.19255.

Tabari, P. *et al.* (2024) 'State-of-the-Art Fast Healthcare Interoperability Resources (FHIR)–Based Data Model and Structure Implementations: Systematic Scoping Review', *JMIR Medical Informatics*, 12(1), p. e58445. Available at: https://doi.org/10.2196/58445.

Taloba, A.I. and Rayan, A. (2025) 'A privacy preserving medical data management framework using blockchain enabled encrypted role based access control', *Scientific Reports*, 15(1), p. 43864. Available at: https://doi.org/10.1038/s41598-025-30916-3.

Taopan, G.I., Boru, M. and Fanggidae, A. (2022) 'Pengamanan Portable Document

UNIVERSITAS
GADJAH MADA
Analisis Komparatif Keamanan Pertukaran Payload Rekam Medis Elektronik Berbasis HL7 FHIR pada Pendekatan SATUSEHAT, AES-GCM 128-Bit dengan ECC, dan CHACHA20-POLY1305
Febriano Ahdan Nadif, Dr. Nur Rokhman, S.Si., M.Kom.; Muhammad Oriza Nurfajri, S.Kom., M.IT.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

Format (PDF) Menggunakan Algoritma Kriptografi Kurva Eliptik', *Jurnal Komputer dan Informatika*, 10(1), pp. 47–54. Available at: https://doi.org/10.35508/jicon.v10i1.5296.

Vorisek, C.N. *et al.* (2022) 'Fast Healthcare Interoperability Resources (FHIR) for Interoperability in Health Research: Systematic Review', *Journal of Medical Internet Research*, 24(7), p. e35724. Available at: https://doi.org/10.2196/35724.

Widodo, B.E. and Purnomo, A.S. (2020) 'IMPLEMENTASI ADVANCED ENCRYPTION STANDARD PADA ENKRIPSI DAN DEKRIPSI DOKUMEN RAHASIA DITINTELKAM POLDA DIY', *Jurnal Teknik Informatika (Jutif)*, 1(2), pp. 69–77. Available at: https://doi.org/10.20884/1.jutif.2020.1.2.21.

Zhang, S. and Singh, M.M. (2026) 'Privacy and Security in Health Big Data: A NIST-Guided Systematic Review of Technologies, Challenges, and Future Directions', *Information*, 17(2), p. 148. Available at: https://doi.org/10.3390/info17020148.