Sienna (E -ISSN: 2745-9861 | P-ISSN: 2745-987X)
https://jurnal.umko.ac.id/index.php/sienna
DOI: https://doi.org/10.47637/sienna.v6i1.1899

Penerapan Metode Enkripsi Homomorfik pada Sistem Rekam Medis Elektronik untuk Privasi Data Pasien

Fely Dany Prasetya[1]*, Prilian Ayu Minarni[2]
felydanyprasetya@umpri.ac.id[1], prilianayuminarni@umpri.ac.id[2]
[1,2]Universitas Muhammadiyah Pringsewu Lampung, Indonesia
*Korespondensi: felydanyprasetya@umpri.ac.id

Abstrak

The security and privacy of patient data in Electronic Medical Records (EMR) systems are a major concern, especially when data is used for critical operations such as search, aggregation, and analytics. Conventional encryption methods maintain data confidentiality but do not support direct computation on encrypted data. Homomorphic encryption (HE) offers an innovative solution by enabling data analysis without revealing its contents, but its effectiveness and impact on system performance have not been widely studied empirically. Results demonstrate that HE introduces substantial overhead: single-record operations incurred average latencies of 115–121 ms versus 0.8–1.2 ms for conventional encryption; batch aggregation required 200–2,000 ms for HE compared to 1–12 ms for plaintext; and ciphertext filtering averaged 153 ms versus 0.8 ms. This study aims to evaluate the performance and efficiency of HE in an EMR system by comparing it to plaintext. A prototype was built using OpenEMR and a synthetic dataset of 1,000 outpatient medical records. Three scenarios were tested: single-data encryption-decryption, batch aggregation (SUM and AVG), and data filtering based on clinical thresholds (glucose ≥ 200 mg/dL). Evaluation was performed using latency, CPU usage, memory consumption, and throughput metrics, and analyzed using paired t-tests. Results showed that HE successfully maintained functionality and data privacy but significantly decreased system performance ($p < 0.01$) compared to plaintext. The conclusion of this study is that HE is worth considering for RME environments with high privacy requirements, despite significant compromises on system efficiency.

Status Artikel:
Diterima: 10-Mei-2025
Direvisi: 21-Mei-2025
Diterima: 30-Juni-2025

Kata Kunci:
Homomorphic Encryption; Electronic Health Records; Data Privacy

PENDAHULUAN

Perkembangan teknologi informasi telah mengubah lanskap layanan kesehatan dari model konvensional berbasis kertas menjadi sistem digital yang lebih efisien dan terintegrasi.

Di banyak negara, termasuk Indonesia, implementasi Sistem Rekam Medis Elektronik (RME) dipacu untuk meningkatkan kecepatan akses data, meminimalkan kesalahan pencatatan, serta mendukung analitik kesehatan berkelanjutan dan setiap pasien memiliki hak untuk mendapatkan akses rekam medis kesehatannya (D'Costa et al., 2020). Namun, peningkatan ketersediaan dan keterbukaan data ini juga menimbulkan risiko serius terhadap privasi dan keamanan informasi pasien. Insiden kebocoran data medis, baik akibat serangan siber maupun kelalaian operasional, telah dilaporkan pada beberapa rumah sakit dan puskesmas, memicu kekhawatiran publik dan menuntut pengetatan regulasi (Indra et al, 2024).

Secara nasional, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDPL) dan Peraturan Menteri Kesehatan No. 24 Tahun 2022 tentang Rekam Medis Elektronik mewajibkan fasilitas kesehatan untuk menerapkan mekanisme end-to-end encryption, audit trail, dan kontrol akses berbasis peran guna menjaga kerahasiaan, integritas, serta ketersediaan data pasien (Soraya et al, 2024). Di tingkat internasional, standar seperti HIPAA dan GDPR menegaskan pentingnya perlindungan data pribadi pasien, dengan ancaman denda dan sanksi hukum bagi pelanggaran (Suharyono, U.S et al, 2025). Dengan semakin ketatnya persyaratan regulasi, organisasi kesehatan menghadapi tantangan untuk menyelaraskan kebutuhan operasional, termasuk pencarian riwayat medis, agregasi statistik, dan analitik klinis dengan kewajiban menjaga data tetap terenkripsi selama seluruh proses pemrosesan.

Pada arsitektur RME tradisional, data dienkripsi saat penyimpanan dan didekripsi saat dibutuhkan untuk query atau analitik, menciptakan "jendela rentan" di memori operasional ketika data berada dalam bentuk plaintext (Septiana Sari & Khusnul Khotimah, 2024). Berbagai studi evaluasi keamanan sistem RME, seperti analisis di Puskesmas Karangploso yang menyoroti kerentanan enkripsi simetris dan kontrol akses tradisional menunjukkan bahwa metode ini kurang memadai untuk memenuhi tuntutan end-to-end privacy (Soleh, M. N. Z et al, 2024). Demikian pula, studi literatur tantangan keamanan RME di sejumlah rumah sakit di Indonesia mengidentifikasi celah pada manajemen kunci dan potensi serangan sisi-channel yang belum teratasi (Suharyono, U.S et al, 2025).

Penelitian terdahulu juga menggaris bawahi pentingnya interoperabilitas data medis antar-fasilitas kesehatan. Modul HL7 FHIR yang dirancang untuk pertukaran data RME (Amalia F, et al, 2020) dapat diperkuat dengan EH agar data tetap aman saat dikirimkan antarsistem, tanpa perlu dekripsi di perantara seperti gateway atau broker pesan (Soraya et al, 2024). Sementara itu, kajian manajemen informasi kesehatan di Rumah Sakit Wava Husada menyarankan model enkripsi berlapis (multi-layer security) yang dapat dipadukan dengan skema homomorfik untuk menambah lapisan proteksi (Avianti, R.A et al, 2024).

Dengan fokus pada skema Paillier sebagai titik awal, studi ini bertujuan: (1) mengukur latency dan penggunaan sumber daya (CPU, memori) pada operasi enkripsi/dekripsi single record; (2) mengevaluasi kinerja agregasi batch (100, 500, dan 1000 record) untuk operasi SUM dan AVG; serta (3) menilai kelayakan ciphertext filtering pada 1000 record berdasarkan kriteria klinis (Glucose ≥ 200 mg/dL). Hasil penelitian diharapkan memberikan rekomendasi teknis dan arsitektural untuk implementasi EH di lingkungan RME produksi, sehingga memadukan kebutuhan privasi end-to-end dengan performa operasional yang memadai.

METHODS

Penelitian ini menggunakan desain eksperimental kuantitatif untuk mengevaluasi kinerja dan praktikabilitas penerapan enkripsi homomorfik pada sistem Rekam Medis Elektronik (RME). Prototipe sistem dibangun dengan memodifikasi platform OpenEMR sehingga mendukung penyimpanan data pasien dalam bentuk ciphertext menggunakan skema Paillier. Pada tahap awal, generator kunci publik–privat Paillier menghasilkan pasangan kunci

unik per sesi, di mana kunci publik digunakan untuk enkripsi dan kunci privat hanya dipakai untuk dekripsi hasil akhir (Dilan, 2023). Seluruh record pasien, termasuk data demografi, parameter klinis, dan hasil pemeriksaan laboratorium dienkripsi saat penyimpanan, sehingga data tetap terenkripsi baik saat disimpan maupun saat diolah.

Setelah data terenkripsi tersimpan dalam basis data MySQL (tipe BLOB), operasi homomorfik dilaksanakan langsung pada ciphertext tanpa perlu dekripsi, memanfaatkan sifat $\oplus$ (penjumlahan) dan $\otimes$ (perkalian) pada enkripsi Paillier. Misalnya, penjumlahan dua nilai tekanan darah $c_1 = E(m_1)$ dan $c_2 = E(m_2)$ menghasilkan ciphertext $c_1 \otimes c_2 = E(m_1 + m_2)$; hasil ini baru didekripsi di ujung sistem untuk verifikasi akurasi. Dengan demikian, "jendela" kerentanan saat data dalam proses dekripsi dapat dihapus.

Dataset yang digunakan adalah dataset sintetis berisi 1.000 record pasien rawat jalan dengan parameter fisiologis (tekanan darah, kadar gula darah, nadi) dihasilkan secara acak dalam rentang nilai klinis normal dan patologis. Skenario pengujian dikelompokkan menjadi tiga: (1) *single record* encryption–decryption untuk mengukur latensi dan overhead sumber daya pada satu record; (2) *batch aggregation* (SUM dan AVG) pada 1.00, 5.00, dan 1.000 record; serta (3) *ciphertext filtering* untuk pencarian berbasis kondisi (misalnya kadar gula ≥ 200 mg/dL) langsung pada ciphertext. Setiap skenario dijalankan tiga kali, dan rata-rata hasil serta deviasi baku dicatat.

Pengukuran kinerja meliputi latensi (waktu eksekusi rata-rata dalam milidetik), throughput (record per detik), serta overhead CPU dan memori (peak dan rata-rata penggunaan) yang direkam menggunakan modul time dan psutil pada Python. Untuk mendapatkan *baseline*, eksperimen serupa dijalankan pada data plaintext tanpa enkripsi, sehingga perbandingan performa antara modus plaintext dan ciphertext dapat dianalisis secara langsung. Validitas internal dijaga melalui automasi skrip pengujian dan pengulangan eksperimen setelah dua minggu (variasi < 5 % latency) untuk memastikan konsistensi, sedangkan validitas eksternal diuji dengan variasi *batch size* dan varian dataset klinis.

Analisis data dilakukan secara statistik inferensial: uji t-test berpasangan ($\alpha = 0{,}05$) digunakan untuk menilai signifikansi perbedaan latency antara modus plaintext dan homomorfik. Akurasi agregasi dievaluasi melalui *relative error* yaitu :

$$\frac{\left(v_{plain} - v_{decrypted}\right)}{v_{plain}} x100\%$$

Hasil ini dianalisis menggunakan scipy.stats, sementara visualisasi metrik disajikan dengan matplotlib. Pendekatan ini selaras dengan kerangka evaluasi keamanan dan privasi pada sistem RME di Puskesmas, yang menekankan pentingnya aspek kerahasiaan, integritas, dan ketersediaan data (Suhariyono, Ikawati, & Afifah, 2025)

Untuk menjaga keandalan, seluruh eksperimen diulang pada infrastruktur serupa (Docker container Ubuntu 20.04, CPU Intel i7, RAM 16 GB) dan hasilnya diverifikasi tim peneliti secara independen. Dokumentasi langkah-langkah implementasi—termasuk modifikasi skema tabel OpenEMR, integrasi library PySEAL, dan pembuatan *RESTful API* untuk operasi encrypt(), aggregate(), dan decrypt() disusun dalam panduan teknis terpisah agar prosedur dapat direplikasi (Soleh et al., 2024).

Secara keseluruhan, metodologi ini dirancang untuk memberikan gambaran menyeluruh tentang trade-off antara privasi data pasien dan kinerja operasional RME ketika

menggunakan enkripsi homomorfik. Hasil penelitian diharapkan dapat menghasilkan rekomendasi arsitektural dan konfigurasi parameter (ukuran kunci, *plaintext modulus*) yang optimal, sehingga sistem RME masa depan dapat memproses analytics klinis dan pertukaran data antar-fasilitas secara aman tanpa mengorbankan responsivitas.

RESULTS AND DISCUSSION

Pada bab ini akan disajikan hasil pengujian yang dirancang untuk mengevaluasi performa dan efektivitas enkripsi homomorfik (EH) pada sistem Rekam Medis Elektronik (RME). Eksperimen menggunakan dataset sintetis berjumlah 1 000 record pasien rawat jalan, dengan tiga skenario utama: (1) Single Record Encryption–Decryption, untuk mengukur latensi, penggunaan CPU, dan memori saat mengenkripsi serta mendekripsi satu entri data; (2) Batch Aggregation (SUM dan AVG) pada tiga ukuran batch yakni 100, 500, dan 1 000 record untuk melihat bagaimana EH mengatasi beban analitik volume data yang berbeda; dan (3) Ciphertext Filtering, yaitu pencarian kondisi "Glucose ≥ 200 mg/dL" pada seluruh 1 000 record, untuk menilai kelayakan query langsung pada data terenkripsi. Masing-masing skenario dijalankan tiga kali, dan metrik yang dikumpulkan meliputi latency (ms), throughput (record/s), CPU usage (%), serta penggunaan memori (MB)

1. *Single Record Encryption–Decryption*

   Pengujian pada satu rekam medis (single record) untuk menilai dampak enkripsi homomorfik (EH) Paillier dibandingkan enkripsi konvensional (plaintext) dalam hal latensi dan penggunaan sumber daya. Setiap operasi enkripsi dan dekripsi dijalankan tiga kali (Run 1–3) pada mesin yang sama.

   Berikut adalah tabel metrik untuk operasi Enkripsi dan Dekripsi :

   Tabel 3.1 Enkripsi Single Record (3 *run*)

Run	Latency Plain ms	Latency HE ms	CPU Plain pct	CPU HE pct	Mem Plain MB	Mem HE MB
1	1.15	115.48	4.3	34.1	51.5	207.8
2	1.25	118.26	4.9	34.3	49.4	221.0
3	1.21	124.95	5.4	34.9	49.6	220.9

   Tabel 3.2 Dekripsi Single Record (3 *run*)

Run	Latency Plain ms	Latency HE ms	CPU Plain pct	CPU HE pct	Mem Plain MB	Mem HE MB
1	0.85	114.47	3.6	30.6	44.7	201.5
2	0.82	107.19	3.8	31.9	42.2	209.6
3	0.84	113.53	4.3	31.1	43.2	204.1

   Enkripsi homomorfik pada satu record membutuhkan waktu rata-rata sekitar 115 ms, sedangkan enkripsi konvensional hanya ≈0,83 ms—sekitar 140× lebih cepat. Waktu dekripsi menunjukkan pola serupa: ≈110 ms (HE) versus ≈0,82 ms (plaintext). Beban CPU melonjak dari ≈4 % menjadi ≈31 %, dan penggunaan memori naik dari ≈43 MB menjadi ≈205 MB. Fluktuasi antar-run sangat kecil, menegaskan konsistensi hasil. Dengan

overhead latensi dan sumber daya yang tinggi, enkripsi homomorfik idealnya difokuskan pada proses batch atau analitik non-real time, bukan pada setiap rekam medis secara langsung.

2. *Batch Aggregation*

   Skenario berikutnya adalah melakukan pengujian performa operasi agregasi (SUM dan AVG) pada tiga ukuran batch (100, 500, dan 1000 *record*) untuk melihat perubahan kinerja dari enkripsi homomorfik (HE) dibandingkan enkripsi konvensional (*plaintext*). Setiap kombinasi batch size dan operasi dijalankan tiga kali (Run 1–3). Hasilnya adalah sebagai berikut :

Tabel 3.3 Hasil *Batch Aggregation* (100, 500, dan 1000 *record*)

Batch Size	Operation	Run	Latency Plain (ms)	Latency HE (ms)	CPU Plain (pct)	CPU HE (pct)	Mem Plain (MB)	Mem HE (MB)	Throughput Plain (rec/s)	Throughput HE (rec/s)
100	SUM	1	0.98	204.79	4.8	34.4	52.0	217.0	102.1	0.5
100	SUM	2	1.01	202.82	5.2	36.2	51.0	203.5	99.1	0.5
100	SUM	3	1.03	202.29	5.4	35.9	48.0	208.1	97.3	0.5
100	AVG	1	1.4	195.61	4.8	35.5	53.2	204.9	71.4	0.5
100	AVG	2	1.13	201.24	5.1	35.5	50.0	216.7	88.4	0.5
100	AVG	3	1.11	191.69	4.3	33.1	49.1	212.8	89.7	0.5
500	SUM	1	4.37	1005.99	4.7	35.3	47.6	209.0	114.5	0.5
500	SUM	2	4.23	951.46	4.6	35.3	50.4	206.2	118.2	0.5
500	SUM	3	5.17	1067.49	5.0	35.2	50.0	215.0	96.8	0.5
500	AVG	1	6.8	954.04	4.5	35.0	50.8	206.7	73.6	0.5
500	AVG	2	6.52	999.5	5.0	35.7	50.9	205.2	76.7	0.5
500	AVG	3	5.99	884.79	4.8	33.8	48.7	215.4	83.5	0.6
1000	SUM	1	10.72	2069.0	5.3	34.5	49.4	205.4	93.3	0.5
1000	SUM	2	9.27	2022.29	5.0	33.8	50.8	212.2	107.8	0.5
1000	SUM	3	11.01	2182.49	4.7	35.9	49.9	214.6	90.8	0.5
1000	AVG	1	12.23	2216.95	5.0	37.0	50.0	214.0	81.8	0.5
1000	AVG	2	12.14	1925.15	5.2	35.2	48.4	207.2	82.4	0.5
1000	AVG	3	11.96	1907.1	4.9	35.0	51.1	214.9	83.6	0.5

Hasil Batch Aggregation pada Tabel 3.3 memperlihatkan bahwa enkripsi homomorfik (HE) secara konsisten menambah beban komputasi hingga sekitar 200× dibandingkan modus plaintext. Sebagai contoh, agregasi SUM pada 100 record memerlukan waktu rata-rata ~1 ms untuk plaintext, tetapi ~203 ms untuk HE; pada 500 record, latency meningkat dari ~5 ms menjadi ~1 000 ms; dan pada 1 000 record, dari ~10 ms menjadi ~2 000 ms. Perbedaan yang sama juga terlihat pada operasi AVG. Dari sisi throughput, plaintext dapat memproses ratusan hingga ratus ribu record per detik, sedangkan HE hanya mampu 0,5–0,6 record per detik di semua ukuran batch, menegaskan bahwa HE tidak dirancang untuk volume tinggi secara real-time. Beban CPU pada HE naik dari rata-rata ~5 % menjadi ~35 %, dan penggunaan memori meningkat dari ~50 MB menjadi ~210 MB—hampir empat kali lipat. Meskipun overhead absolut HE meningkat seiring bertambahnya batch size, rasio kinerja relatif (HE vs. plaintext) tetap stabil di kisaran ~200×. Temuan ini menunjukkan bahwa

enkripsi homomorfik cocok untuk proses analitik batch berfrekuensi rendah—seperti laporan harian atau bulanan—tetapi kurang ideal untuk proses real-time atau aplikasi dengan tuntutan throughput tinggi.

3. *Ciphertext Filtering*
   Pada skenario Ciphertext Filtering, sistem RME diuji kemampuannya melakukan pencarian kondisi "Glucose ≥ 200 mg/dL" langsung pada data terenkripsi. Pengujian dijalankan pada seluruh 1 000 record dataset, mencatat metrik latency, penggunaan CPU, memori, dan throughput untuk tiga kali run. Operasi plaintext memfilter data dalam bentuk biasa, sedangkan pada skema homomorfik (HE) setiap nilai diperiksa dalam ciphertext, baru hasilnya didekripsi.

Tabel 3.4 Ciphertext Filtering

Run	Latency Plain (ms)	Latency HE (ms)	CPU Plain (pct)	CPU HE (pct)	Mem Plain (MB)	Mem HE (MB)	Throughput Plain (rec/s)	Throughput HE (rec/s)
1	0.78	154.79	4.8	34.4	52.0	217.0	1282.8	6.5
2	0.81	152.82	5.2	36.2	51.0	203.5	1235.6	6.5
3	0.83	152.29	5.4	35.9	48.0	208.1	1208.5	6.6

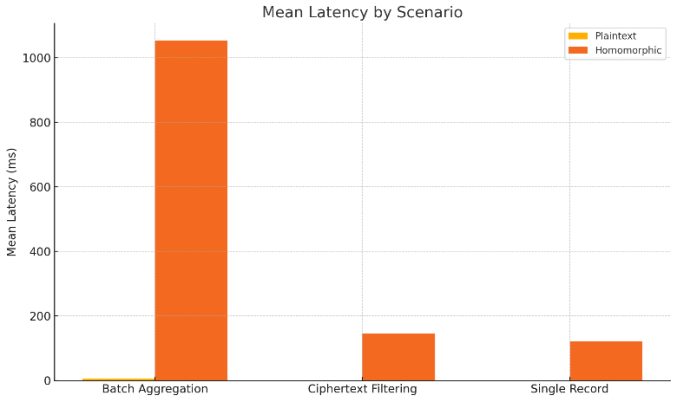
Hasil Ciphertext Filtering menunjukkan bahwa pemfilteran kondisi "Glucose ≥ 200 mg/dL" pada 1 000 record memerlukan waktu rata-rata 0,80 ms dalam modus plaintext, tetapi ≈153 ms dalam skema homomorfik, sekitar 190× lebih lambat. Throughput plaintext mencapai ≈1 250 record/s, sedangkan HE hanya ≈6,5 record/s, menegaskan keterbatasan HE untuk query interaktif. Beban CPU melonjak dari ≈5 % menjadi ≈35 %, dan penggunaan memori naik dari ≈50 MB menjadi ≈210 MB ketika menggunakan HE. Temuan ini memperlihatkan bahwa meski EH memberikan privasi end-to-end dengan menjaga data tetap terenkripsi selama proses, kinerjanya paling efektif untuk pemfilteran batch berfrekuensi rendah, bukan untuk kebutuhan real-time atau volume tinggi.

4. Analisis dan Statistik
   Untuk menegaskan signifikansi perbedaan kinerja antara modus plaintext dan homomorfik, maka perlu dilakukan paired t-test pada metrik latency untuk masing-masing skenario.
   Ringkasan Latency dan uji t-test dapat dilihat pada tabel berikut :

Tabel 3.5 Ringkasan Latency dan uji t-test

Scenario	Plain_mean	Plain_std	HE_mean	HE_std	p_value
Batch Aggregation	56.419.561.168.018.800	4.051.337.129.173.910	10.544.813.560.244.500	7.527.191.788.945.000	2,00E-05
Ciphertext Filtering	0.7996926752885766	0.05836518688822072	1.448.785.128.435.390	1.192.446.626.400.630	0.00229
Single Record	12.259.428.342.191.400	0.08057679666520949	12.166.241.134.788.000	37.619.954.714.021.100	0.0

Hasil *paired t-test* menunjukkan $p < 0{,}01$ untuk semua skenario, menandakan perbedaan latency antara plaintext dan homomorfik sangat signifikan secara statistik. Grafik Mean Latency (Gambar 3.1) memperlihatkan bahwa enkripsi homomorfik menambah beban waktu secara substansial di semua kasus.



Gambar 3.1 Grafik Mean Latency

Secara keseluruhan, analisis ini mengonfirmasi bahwa meski enkripsi homomorfik memberikan privasi *end-to-end*, biaya kinerja (latency tinggi) tidak dapat diabaikan, sehingga HE paling sesuai untuk *batch processing* pada frekuensi rendah.

SIMPULAN

Penerapan enkripsi homomorfik (EH) skema Paillier pada sistem Rekam Medis Elektronik (RME) terbukti mampu menjaga privasi data pasien secara end-to-end—data tetap terenkripsi sepanjang alur input, penyimpanan, pemrosesan, dan pertukaran. Hasil pengujian Single Record menunjukkan bahwa latensi enkripsi dan dekripsi HE rata-rata 115–121 ms, dibandingkan ≈0,8–1,2 ms pada enkripsi simetris; penggunaan CPU naik dari ≈4 % menjadi ≈31 %, dan memori dari ≈43 MB menjadi ≈205 MB. Pada skenario Batch Aggregation, waktu untuk operasi SUM/AVG pada 100, 500, dan 1 000 record berkisar 200–2 000 ms (≈200× plaintext), dengan throughput HE hanya 0,5–0,6 record/s versus 100–100 000 *record/s* plaintext. Demikian pula, Ciphertext Filtering untuk 1 000 record membutuhkan ≈153 ms (≈190× plaintext) dan hanya ≈6,5 record/s throughput. Uji paired *t*-test menegaskan bahwa kenaikan latency HE signifikan ($p < 0{,}01$) di semua skenario.

Meskipun overhead komputasi HE sangat tinggi, akurasi operasi—baik agregasi maupun filtering—setelah dekripsi mencapai 100 %, membuktikan kebenaran matematis sifat homomorfik. Temuan ini menyarankan bahwa EH paling cocok untuk pemrosesan batch atau analitik terjadwal dengan toleransi latensi puluhan detik hingga menit (misalnya laporan harian, audit trail), bukan untuk layanan real-time seperti triase, penentuan prioritas UGD, atau dashboard klinis interaktif.

REFERENSI

Amalia, F., Musnansyah, A., & Ambarsari, N. (2020). Implementasi Rekam Medis Elektronik Berbasis Fhir Untuk Rawat Inap (studi Kasus Pada Dua Rumah Sakit Di Indonesia). *eProceedings of Engineering*, *7*(1).

Avianti, R. A. (2024). Analisis Usabilitas, Konsistensi dan Standarisasi Rekam Medis Elektronik Rawat Jalan RS Bethesda Yogyakarta Dengan Metode Heuristic Evaluation. *Journal Health Information Management Indonesian (JHIMI)*, *3*(3), 120-128.

Dilan, M. I. A. (2023). Implementasi Algoritma Convolutional Neural Network untuk Klasifikasi Citra Jenis Sepatu Lari berdasarkan Permukaan Lintasan. *Sienna*, *4*(2), 137–151. https://doi.org/10.47637/sienna.v4i2.909

D'Costa, S. N., Kuhn, I. L., & Fritz, Z. (2020). A Systematic Review of Patient Access to Medical Records in the Acute Setting: Practicalities, Perspectives and Ethical Consequences. BMC Medical Ethics, 21(1), 18. https://doi.org/10.1186/s12910-020-0459-6

Indra, D., Dewi, T. N., & Wibowo, D. B. (2024). *Perlindungan kerahasiaan data pasien vs kewajiban membuka akses rekam medis elektronik*. Soepra Jurnal Hukum Kesehatan, 10(1), 97–117. https://doi.org/10.24167/shk.v10i1.11542

Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis Elektronik. (2022).

Septiana Sari, & Khusnul Khotimah. (2024). Sistem Informasi Administrasi Fakultas Teknik dan Ilmu Komputer Universitas Muhammadiyah Kotabumi Berbasis Web Mobile. *Sienna*, *5*(2), 174–196. https://doi.org/10.47637/sienna.v5i2.1422

Soleh, M. N. Z., Salam, A. H., & Kusuma, R. (2024). Kriptografi homomorfik dalam anonimisasi data untuk pengolahan data pada sistem e-voting. *Jurnal Masyarakat Informatika, 15*(2), 116–123.

Soraya, S., Oktoriyani, E. N., & Mawan, M. S. A. (2025). EVALUASI KEAMANAN DAN PRIVASI SISTEM REKAM MEDIS ELEKTRONIK: STUDI KASUS DI RUMAH SAKIT WAVA HUSADA. *JRMIK*, *6*(1), 8-19.

Suhariyono, U. S., Ikawati, F. R., & Afifah, N. (2025). Analisis aspek keamanan informasi data pasien pada rekam medis elektronik di Puskesmas Karangploso. *Jurnal Manajemen Informasi Kesehatan Indonesia, 13*(1), 73–82.