

Evaluasi Keamanan Data Dalam Sistem Rekam Medis Elektronik Di Rumah Sakit Umum Daerah Banyumas

Duanda Cesar Palupi¹, Ilham Rahmansyah², Khusnul Khotimah Arum³,

^{1,2,3}Program Studi Rekam Medis Dan Informasi Kesehatan, Politeknik Yakpermas Banyumas

duandacesar55@gmail.com , iam.rahmansyah@gmail.com , arumgusta@gmail.com

Keywords:

*Data security,
Electronic,
Medical Record,
RSUD Banyumas.*

ABSTRACT

This study aims to evaluate data security in the Electronic Medical Record (EMR) system at Banyumas Regional General Hospital based on three main aspects: confidentiality, integrity, and availability. This research employed a qualitative approach with data collected through interviews, observations, and documentation involving registration staff, medical record officers, and the IT department. The findings indicate that, in terms of confidentiality, the hospital has implemented personal usernames and passwords as well as an automatic logout feature; however, regular password updates have not yet been enforced, which increases the risk of unauthorized access. Regarding integrity, data management is supported by access restrictions based on job roles and user activity logs, although routine monitoring and periodic data audits still need improvement. In terms of availability, the EMR system performs automatic backups three times a day and provides fast access to patient data, yet a written Standard Operating Procedure (SOP) for data breach handling is not available. Furthermore, although general SOPs for EMR implementation exist, training on data security and routine evaluations remain limited. Overall, data security in the EMR system at Banyumas Regional General Hospital is considered adequate, but strengthening policies, staff education, and supervision is necessary to ensure optimal data protection and alignment with information security standards.

Kata Kunci

*Keamanan Data,
Rekam Medis,
Elektronik,
RSUD Banyumas.*

ABSTRAK

Penelitian ini bertujuan mengevaluasi keamanan data dalam Sistem Rekam Medis Elektronik (RME) di Rumah Sakit Umum Daerah Banyumas berdasarkan tiga aspek utama, yaitu kerahasiaan, integritas, dan ketersediaan. Penelitian menggunakan pendekatan kualitatif dengan teknik pengumpulan data melalui wawancara, observasi, dan dokumentasi terhadap petugas pendaftaran, kesmik, dan bagian IT. Hasil penelitian menunjukkan bahwa pada aspek kerahasiaan, RSUD Banyumas telah menerapkan penggunaan username dan password personal serta fitur automatic logout, namun kebijakan pembaruan kata sandi secara berkala belum diterapkan sehingga meningkatkan risiko akses tidak sah. Pada aspek integritas, pengelolaan data sudah didukung dengan pembatasan hak akses sesuai tupoksi dan pencatatan aktivitas pengguna melalui user log, meskipun pengawasan rutin dan audit data masih perlu diperkuat. Dari aspek ketersediaan, sistem RME telah memiliki mekanisme backup otomatis tiga kali sehari serta akses data yang cepat, namun belum terdapat SOP tertulis mengenai penanganan insiden kebocoran data. Selain itu, SOP umum terkait penyelenggaraan RME telah tersedia, tetapi implementasi pelatihan keamanan data dan evaluasi berkala masih terbatas. Secara keseluruhan, keamanan data dalam RME di RSUD Banyumas sudah berjalan cukup baik, namun peningkatan kebijakan, edukasi, serta pengawasan perlu dilakukan agar perlindungan data pasien lebih optimal dan sesuai standar keamanan informasi.

Korespondensi Penulis:

Khusnul Khotimah Arum
Politeknik Yakpermas Banyumas
Telepon : +628221935921
Email: arumgusta@gmail.com

1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transformasi digital di berbagai sektor, termasuk sektor kesehatan. Pemanfaatan Sistem Informasi Kesehatan (SIK) menjadi salah satu strategi untuk meningkatkan efektivitas, efisiensi, dan kualitas pelayanan kesehatan. Dalam lingkungan rumah sakit, penerapan Sistem Informasi Manajemen Rumah Sakit (SIMRS) berperan penting dalam mengintegrasikan proses administrasi, keuangan, pelayanan medis, serta pengelolaan data pasien secara terpusat. Sistem yang terintegrasi memungkinkan informasi tersedia secara cepat, akurat, dan berkesinambungan sehingga dapat mendukung pengambilan keputusan manajerial maupun klinis (Kementerian Kesehatan RI, 2022; Hatta, 2017; World Health Organization, 2021).

Sejalan dengan perkembangan SIMRS, pemerintah Indonesia mewajibkan seluruh fasilitas pelayanan kesehatan untuk menyelenggarakan Rekam Medik Elektronik (RME) sebagaimana diatur dalam Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medik. Regulasi tersebut menegaskan bahwa RME merupakan bagian dari sistem informasi fasilitas pelayanan kesehatan yang bertujuan meningkatkan mutu pelayanan, menjamin keamanan dan kerahasiaan data, serta mewujudkan pengelolaan rekam medis yang berbasis digital dan terintegrasi. Selain meningkatkan efisiensi pelayanan, RME juga mampu mempercepat akses informasi pasien, mengurangi kesalahan pencatatan, serta mendukung kesinambungan pelayanan kesehatan.

Dalam implementasinya, keamanan data menjadi aspek yang sangat penting karena rekam medis mengandung informasi pribadi dan kesehatan pasien yang bersifat rahasia. Berdasarkan Permenkes Nomor 24 Tahun 2022, keamanan RME harus memenuhi prinsip kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Kerahasiaan menjamin bahwa data hanya dapat diakses oleh pihak yang berwenang, integritas memastikan data tetap akurat dan tidak mengalami perubahan tanpa izin, sedangkan ketersediaan menjamin data dapat diakses ketika dibutuhkan dalam proses pelayanan kesehatan. Ketiga prinsip tersebut menjadi dasar dalam pengelolaan keamanan informasi kesehatan di era digital.

Meskipun digitalisasi pelayanan kesehatan memberikan berbagai manfaat, peningkatan penggunaan teknologi informasi juga meningkatkan risiko keamanan data. Ancaman seperti malware, ransomware, pencurian identitas, penyalahgunaan hak akses, dan kebocoran data menjadi tantangan yang harus dihadapi oleh rumah sakit. Selain faktor teknologi, risiko keamanan juga dapat berasal dari faktor manusia, seperti penggunaan kata sandi yang lemah, kurangnya kesadaran keamanan informasi, dan ketidakpatuhan terhadap prosedur operasional. Oleh karena itu, diperlukan sistem keamanan informasi yang mampu melindungi data pasien secara menyeluruh melalui kombinasi kebijakan, teknologi, dan sumber daya manusia yang kompeten.

Berbagai penelitian terdahulu telah mengkaji keamanan data pada sistem Rekam Medik Elektronik. Kruse et al. (2017) menemukan bahwa ancaman utama terhadap keamanan RME berasal dari faktor manusia, lemahnya kontrol akses, dan kurangnya pelatihan keamanan informasi bagi pengguna sistem. Almulhim dan Traore (2020) menyatakan bahwa penerapan autentikasi pengguna, audit akses, dan pengendalian hak akses berperan penting dalam menjaga kerahasiaan data pasien. Sementara itu, penelitian lain menunjukkan bahwa penerapan standar keamanan informasi seperti ISO/IEC 27001 dapat membantu organisasi kesehatan dalam mengidentifikasi risiko keamanan serta meningkatkan efektivitas pengendalian keamanan informasi.

Namun demikian, penelitian terdahulu umumnya hanya berfokus pada aspek teknis keamanan sistem atau tingkat kepatuhan terhadap regulasi tanpa mengkaji secara komprehensif keterkaitan antara teknologi, kebijakan organisasi, dan sumber daya manusia. Selain itu, masih terbatas penelitian yang secara khusus mengevaluasi keamanan data Rekam Medik Elektronik pada rumah sakit pemerintah daerah menggunakan pendekatan ISO/IEC 27001:2013. Hingga saat ini, penelitian mengenai implementasi keamanan data RME di RSUD Banyumas juga masih relatif terbatas sehingga kondisi aktual keamanan informasi pada rumah sakit tersebut belum tergambarkan secara menyeluruh.

Berdasarkan kesenjangan penelitian tersebut, novelty (kebaruan) penelitian ini terletak pada

evaluasi keamanan data Rekam Medis Elektronik di RSUD Banyumas menggunakan kerangka kerja ISO/IEC 27001:2013 dengan mengintegrasikan aspek teknologi, kebijakan keamanan informasi, pengelolaan sumber daya manusia, serta kepatuhan terhadap regulasi kesehatan. Pendekatan ini diharapkan mampu memberikan gambaran yang lebih komprehensif mengenai tingkat keamanan data RME dan menghasilkan rekomendasi perbaikan yang sesuai dengan kondisi RSUD Banyumas.

Tujuan penelitian ini adalah untuk menganalisis penerapan keamanan data pada sistem Rekam Medis Elektronik di RSUD Banyumas, mengidentifikasi potensi risiko dan kelemahan keamanan yang masih terdapat dalam sistem, serta mengevaluasi kesesuaian implementasi keamanan informasi berdasarkan standar ISO/IEC 27001:2013. Hasil penelitian diharapkan dapat menjadi bahan evaluasi dan rekomendasi dalam meningkatkan keamanan data pasien serta mendukung keberhasilan transformasi digital pelayanan kesehatan di RSUD Banyumas.

2. METODE PENELITIAN

2.1 Jenis Penelitian

Penelitian ini menggunakan metode penelitian kualitatif dengan pendekatan deskriptif (Sugiyono, 2022). Metode penelitian kualitatif digunakan untuk memahami fenomena yang terjadi secara mendalam berdasarkan perspektif informan yang terlibat dalam penelitian (Moleong, 2021). Pendekatan deskriptif bertujuan untuk menggambarkan kondisi yang terjadi secara sistematis dan faktual sesuai dengan keadaan di lapangan (Creswell & Creswell, 2018). Penelitian ini dilakukan di RSUD Banyumas untuk menganalisis penerapan keamanan data pada sistem Rekam Medis Elektronik berdasarkan standar ISO/IEC 27001:2013 (International Organization for Standardization [ISO], 2013).

2.2 Subyek Penelitian

Subjek penelitian merupakan individu yang memberikan informasi terkait fokus penelitian (Sugiyono, 2022). Informan dalam penelitian ini berjumlah 11 orang yaitu seluruh tenaga kerja yang bekerja di Rumah Sakit Umum Daerah Banyumas yang terdiri dari 6 anggota pendaftaran, 4 anggota kesmik, dan 1 orang bagian IT. Pemilihan informan dilakukan menggunakan teknik purposive sampling karena informan dipilih berdasarkan pengetahuan dan keterlibatannya terhadap objek penelitian (Yusuf, 2017). Teknik purposive sampling memungkinkan peneliti memperoleh data yang sesuai dengan tujuan penelitian (Sugiyono, 2022).

2.3 Pengumpulan Data

Pengumpulan data dilakukan menggunakan data primer yang diperoleh melalui wawancara, observasi, dan dokumentasi (Sugiyono, 2022). Wawancara dilakukan secara mendalam untuk memperoleh informasi mengenai penerapan keamanan data pada sistem Rekam Medis Elektronik (Creswell & Creswell, 2018). Observasi dilakukan untuk mengamati secara langsung aktivitas penggunaan sistem dan penerapan prosedur keamanan informasi di rumah sakit (Moleong, 2021). Dokumentasi dilakukan dengan menelaah dokumen yang berkaitan dengan keamanan data, seperti standar operasional prosedur, kebijakan keamanan informasi, dan dokumen pendukung lainnya (Sugiyono, 2022). Penggunaan berbagai teknik pengumpulan data bertujuan memperoleh informasi yang lebih lengkap dan meningkatkan kualitas hasil penelitian (Creswell & Creswell, 2018).

2.4 Analisis Data

Analisis data merupakan proses mengorganisasi dan menginterpretasikan data untuk menjawab rumusan masalah penelitian (Miles et al., 2014). Analisis data dalam penelitian ini dilakukan melalui tahap reduksi data, penyajian data, dan penarikan kesimpulan (Miles et al., 2014). Reduksi data dilakukan dengan memilih dan memfokuskan data yang relevan dengan tujuan penelitian (Miles et al., 2014). Penyajian data dilakukan dalam bentuk uraian naratif untuk mempermudah proses interpretasi hasil penelitian (Sugiyono, 2022). Penarikan kesimpulan dilakukan berdasarkan pola dan hubungan yang ditemukan dari hasil analisis data (Miles et al., 2014).

Hasil wawancara, observasi, dan dokumentasi dianalisis menggunakan kerangka kerja ISO/IEC 27001:2013 sebagai standar manajemen keamanan informasi (ISO, 2013). Analisis difokuskan pada aspek pengendalian akses, keamanan sumber daya manusia, keamanan operasional, dan pengelolaan keamanan informasi yang berkaitan dengan Rekam Medis Elektronik (ISO, 2013). Penggunaan ISO/IEC 27001:2013 bertujuan untuk menilai kesesuaian penerapan keamanan data di RSUD Banyumas dengan standar internasional keamanan informasi (ISO, 2013).

Keabsahan data diuji menggunakan teknik triangulasi sumber dan triangulasi metode (Moleong, 2021). Triangulasi sumber dilakukan dengan membandingkan informasi yang diperoleh dari setiap informan penelitian (Sugiyono, 2022). Triangulasi metode dilakukan dengan membandingkan hasil wawancara, observasi, dan dokumentasi yang diperoleh selama penelitian (Creswell & Creswell, 2018). Penggunaan triangulasi bertujuan meningkatkan kredibilitas dan kepercayaan terhadap hasil penelitian (Moleong, 2021).

3. HASIL DAN ANALISIS

3.1 Menganalisis Aspek Keamanan Dalam Sistem Rekam Medis Elektronik Di RSUD Banyumas Berdasarkan Aspek Kerahasiaan (*confidentiality*)

Aspek kerahasiaan (*confidentiality*) berperan penting dalam melindungi informasi pasien agar tidak dapat diakses oleh pihak yang tidak berwenang. Pengelolaan dan distribusi data rekam medis secara elektronik memiliki potensi risiko penyalahgunaan yang dapat menimbulkan kerugian bagi pasien apabila tidak disertai dengan sistem pengamanan yang memadai. Kerahasiaan merupakan bentuk perlindungan terhadap data dan informasi dari ancaman pihak internal maupun eksternal yang tidak memiliki hak akses, sehingga informasi yang tersimpan dalam rekam medis elektronik tetap terjaga keamanan, penggunaan, dan penyebarannya. Berdasarkan hasil penelitian mengenai keamanan informasi dalam penerapan rekam medis elektronik, diperoleh temuan dari wawancara dengan responden sebagai berikut.

“Setiap petugas memiliki username dan password pribadi, dan akses hanya dapat digunakan di area jaringan internal”

Berdasarkan hasil wawancara dan observasi di ketahui setiap petugas memiliki *username* dan *password* masing-masing untuk membuktikan bahwa pengguna memiliki wewenang untuk masuk kedalam sistem untuk menghindari percobaan pengaksesan dari pengguna yang tidak memiliki wewenang dan RME hanya dapat digunakan di area jaringan internal rumah sakit. Menjaga dengan menggunakan *password* masih banyak kelemahan, terutama pengguna masih menggunakan *password* yang lemah

Dari hasil wawancara dengan responden diketahui bahwa penggunaan *password* di sistem RME belum menggunakan karakter khusus. berikut adalah kutipan hasil wawancara dengan responden

“Ya ada setiap petugas punya username dan password masing-masing kalo untuk pergantian password belum ada tetapi petugas bisa mengganti mengganti secara mandiri”

“Semua petugas bisa mengakses dan menunya dibedakan sesuai kebutuhan petugas”

“Setiap petugas memiliki username dan password pribadi, dan akses hanya dapat digunakan di area jaringan internal rumah sakit. Selain itu, sistem juga sudah memiliki fitur logout otomatis jika tidak aktif selama beberapa waktu”

Hasil wawancara di atas menunjukkan bahwa setiap petugas memiliki *username* dan *password* pribadi serta akses terbatas di jaringan internal. Sistem sudah memiliki fitur logout otomatis, namun belum ada pergantian *password* berkala. Hak akses dibedakan sesuai jabatan. Aspek kerahasiaan sudah cukup baik tetapi perlu peningkatan pada keamanan akun.

3.2 Menganalisis Aspek Keamanan Dalam Sistem Rekam Medis Elektronik Di RSUD Banyumas Berdasarkan Aspek Integritas(*integrity*)

Aspek integritas (*integrity*) berkaitan dengan upaya menjaga keakuratan, kelengkapan, dan konsistensi data rekam medis agar tetap sesuai dengan kondisi sebenarnya. Dalam penerapan rekam medis elektronik, integritas data menjadi hal yang sangat penting untuk mencegah terjadinya perubahan, penghapusan, maupun manipulasi data oleh pihak yang tidak berwenang. Integritas data menjamin bahwa informasi yang tersimpan dan digunakan dalam pelayanan kesehatan dapat dipercaya serta tidak mengalami distorsi selama proses penyimpanan, pengolahan, dan distribusi. Berdasarkan hasil penelitian terkait keamanan informasi dalam penerapan rekam medis elektronik, diperoleh hasil wawancara dengan responden sebagai berikut.

“Kesalahan input data kadang terjadi, namun segera dikoreksi melalui fitur edit data oleh petugas yang berwenang dengan mencantumkan alasan perubahan”

“Dari aksesnya karena yang dapat mengubah data pasien hanya bagian petugas rekam medis”

“Sudah karena sebelumnya dari pihak it menyesuaikan dengan kebutuhan petugasnya”

Hasil wawancara di atas kesalahan data pasien memang terkadang terjadi, namun segera ditangani oleh petugas yang berwenang untuk keamanan dan integritas data pasien setiap akun pengguna memiliki hak yang terbatas sesuai dengan tugasnya dan format data dalam sistem telah disesuaikan dengan standar kementerian Kesehatan

3.3 Menganalisis Aspek Keamanan Dalam Sistem Rekam Medis Elektronik Di RSUD Banyumas Berdasarkan Aspek Ketersediaan(*Availability*)

Aspek ketersediaan (*availability*) berkaitan dengan jaminan bahwa data dan informasi rekam medis elektronik dapat diakses secara tepat waktu oleh pengguna yang berwenang ketika dibutuhkan. Ketersediaan informasi sangat penting dalam mendukung kelancaran pelayanan kesehatan, terutama dalam proses pengambilan keputusan medis. Gangguan sistem, kerusakan perangkat, maupun masalah jaringan dapat menghambat akses terhadap data rekam medis dan berpotensi memengaruhi mutu pelayanan. Oleh karena itu, diperlukan pengelolaan sistem yang baik agar data rekam medis elektronik tetap tersedia secara berkelanjutan. Berdasarkan hasil penelitian terkait keamanan informasi dalam penerapan rekam medis elektronik, diperoleh hasil wawancara dengan responden sebagai berikut.

“backup data dilakukan setiap hari pada jam pada jam 18.00, 21.00 dan jam 01.00 dini hari”

“Akses data pasien dapat dilakukan dalam hitungan detik, selama jaringan rumah sakit stabil dan tidak ada gangguan sistem”

“wah kalo itu belum ada prosedurnya karena selama ini belum pernah terjadi”

Hasil wawancara di atas menunjukkan bahwa sistem melakukan *backup* data tiga kali sehari dan akses data pasien cepat selama jaringan stabil. Namun, prosedur kebocoran data belum tersedia. Ketersediaan sistem sudah baik, hanya perlu SOP penanganan insiden.

3.4 Menganalisis Aspek Keamanan Dalam Sistem Rekam Medik Elektronik Di RSUD Banyumas Berdasarkan Aspek SOP dan Peangawasan Keamanan

Aspek standar operasional prosedur (SOP) dan pengawasan keamanan berperan penting dalam memastikan penerapan keamanan informasi rekam medis elektronik berjalan sesuai dengan ketentuan yang berlaku. SOP menjadi pedoman bagi petugas dalam mengelola, mengakses, dan melindungi data rekam medis elektronik agar terhindar dari kesalahan maupun penyalahgunaan. Selain itu, pengawasan keamanan diperlukan untuk memantau kepatuhan pengguna terhadap SOP yang telah ditetapkan serta mendeteksi potensi pelanggaran keamanan informasi. Dengan adanya SOP yang jelas dan pengawasan yang berkelanjutan, keamanan data rekam medis elektronik dapat lebih terjamin. Berdasarkan hasil penelitian terkait keamanan informasi dalam penerapan rekam medis elektronik, diperoleh hasil wawancara dengan responden sebagai berikut.

“Rumah sakit telah memiliki SOP penggunaan dan keamanan sistem RME, yang mengatur hak akses, hingga prosedur penanganan gangguan”

“Kalo pelatihannya ada tergantung dari sistem apa yang kan di kembangkan”

“Sudah waktunya 30 menit jika tidak ada tidak digunakan oleh petugas”

Hasil wawancara di atas menunjukkan bahwa RSUD Banyumas memiliki SOP penggunaan RME dan fitur *logout* otomatis 30 menit. Petugas sudah mendapat pelatihan penggunaan, namun belum ada pelatihan khusus keamanan data penerapan SOP cukup baik, namun masih perlu peningkatan pemahaman keamanan

KESIMPULAN

A. Saran

Saran yang dapat diberikan adalah RSUD Banyumas perlu menyusun SOP khusus terkait penanganan insiden keamanan informasi dan kebocoran data, melakukan audit serta evaluasi keamanan sistem secara berkala, dan meningkatkan pelatihan keamanan informasi bagi seluruh pengguna sistem. Selain itu, penelitian selanjutnya disarankan melibatkan jumlah informan yang lebih banyak serta melakukan analisis berdasarkan seluruh kontrol keamanan dalam standar ISO/IEC 27001:2013 agar diperoleh gambaran yang lebih komprehensif mengenai tingkat keamanan Rekam Medik Elektronik di rumah sakit.

B. Implikasi

Penelitian ini menunjukkan bahwa penerapan keamanan data yang baik pada sistem RME dapat mendukung perlindungan informasi kesehatan pasien, meningkatkan kepercayaan pengguna

terhadap sistem informasi rumah sakit, serta mendukung keberlangsungan pelayanan kesehatan yang efektif dan berkelanjutan. Temuan penelitian ini juga dapat menjadi bahan evaluasi bagi manajemen rumah sakit dalam memperkuat tata kelola keamanan informasi sesuai standar ISO/IEC 27001:2013.

Berdasarkan hasil penelitian, penerapan keamanan data pada Sistem Rekam Medis Elektronik (RME) di RSUD Banyumas telah memenuhi aspek kerahasiaan, integritas, dan ketersediaan data. Kerahasiaan data pasien dijaga melalui penggunaan username dan password pribadi serta fitur logout otomatis, sedangkan integritas data terjamin karena perubahan data hanya dapat dilakukan oleh petugas yang berwenang sesuai prosedur yang berlaku. Dari aspek ketersediaan, sistem telah didukung oleh mekanisme backup data otomatis yang dilakukan secara berkala sehingga data dapat diakses dengan cepat saat dibutuhkan. Selain itu, RSUD Banyumas telah memiliki Standar Operasional Prosedur (SOP) penggunaan dan keamanan sistem RME sebagai pedoman dalam pengelolaan keamanan informasi. Namun, penelitian ini juga menemukan bahwa belum terdapat SOP khusus yang mengatur penanganan insiden kebocoran data atau gangguan keamanan informasi.

Implikasi penelitian ini menunjukkan bahwa penerapan keamanan data yang baik pada sistem RME dapat mendukung

REFERENSI

- [1] Almulhim, A., & Traore, I. (2020). Electronic health record security and privacy: Challenges and opportunities. *Health Policy and Technology*, 9(2), 122–131.
- [2] Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.
- [3] Direktorat Jenderal Pelayanan Kesehatan, *Petunjuk Teknis Penggunaan Anggaran dalam Penyelenggaraan Jejaring Pengampunan Pelayanan Kesehatan Prioritas*, 2024.
- [4] Firmansyah, R. Subekti, N. Purwandari, and R. Karepesina, "Implementasi Algoritma Keamanan Data Berbasis Enkripsi Pada Platform Cloud Computing Untuk Pembelajaran di SMK Cipta Insani Mandiri," *Journal of Data Analytics, Information, and Computer Science*, vol. 2, no. 1, pp. 81–96, 2025, doi: 10.70248/jdaics.v2i1.1804.
- [5] H. Fitriani and R. Sulastri, "Pengaruh Luas Lahan dan Penggunaan Sarana Produksi terhadap Produktivitas Kentang di Kabupaten Garut," *Jurnal Agribisnis dan Pertanian*, vol. 8, no. 1, pp. 45–52, 2020.
- [6] Hatta, G. R. (2017). *Pedoman Manajemen Informasi Kesehatan di Sarana Pelayanan Kesehatan*. Jakarta: Universitas Indonesia Press.
- [7] International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information Technology—Security Techniques—Information Security Management Systems—Requirements*. Geneva: ISO.
- [8] International Organization for Standardization. (2013). *ISO/IEC 27001:2013 information technology—Security techniques—Information security management systems—Requirements*. ISO.
- [9] K. Hasegawa et al., "Cybersecurity Interventions in Health Care Organizations in Low- and Middle-Income Countries: Scoping Review," *Journal of Medical Internet Research*, vol. 26, no. 1, pp. 1–15, 2024, doi: 10.2196/47311.
- [10] Kementerian Kesehatan Republik Indonesia. (2022). *Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis*. Jakarta: Kementerian Kesehatan Republik Indonesia.
- [11] Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of Medical Systems*, 41(8), 127.
- [12] L. Dzamesi and N. Elsayed, "A Review on the Security Vulnerabilities of the IoMT against Malware Attacks and DDoS," *arXiv preprint*, 2025.
- [13] L. E. Hutagalung, "Analisa Manajemen Risiko Sistem Informasi Manajemen Rumah Sakit (SIMRS) pada Rumah Sakit XYZ Menggunakan ISO 31000," *TelKa*, vol. 12, no. 1, pp. 23–33, 2022, doi: 10.36342/teika.v12i01.2820.
- [14] M. Cahyani, L. Syafanny, S. Kamil, K. Mukharama, and D. Sutha, "Tinjauan Literatur: Peran Rekam Medis Berbasis Elektronik Terhadap Pelayanan Kesehatan," *Jurnal Manajemen Informasi Kesehatan Indonesia*, vol. 12, pp. 155–159, 2024, doi: 10.33560/jmiki.v12i2.648.
- [15] M. Hussain, S. Anwar, and S. Huang, "Socioeconomic and Demographic Factors Affecting Labor Force Participation in Pakistan," *Journal of Sustainable Development*, vol. 9, no. 4, 2016, doi: 10.5539/jsd.v9n4p70.
- [16] Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE Publications.
- [17] Moleong, L. J. (2021). *Metodologi penelitian kualitatif (Edisi revisi)*. PT Remaja Rosdakarya.

- [18] N. Dewi and A. V. Ricky, "Analisis Penerapan Audit Trail Pada Rekam Medis Elektronik di Rumah Sakit X Jawa Tengah," *Jurnal Ners*, vol. 9, no. 8, pp. 4228–4236, 2025.
- [19] P. A. Danarrahmanto, "Pengaruh Rekam Medis Elektronik Terhadap Loyalitas Pasien di Tami Dental Care," *Jurnal Manajemen Informasi Kesehatan Indonesia*, vol. 9, no. 2, p. 151, 2021, doi: 10.33560/jmiki.v9i2.332.
- [20] P. Ewoh and T. Vartiainen, "Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review," *Journal of Medical Internet Research*, vol. 26, 2024, doi: 10.2196/46904.
- [21] R. C. Irawan, S. Windarti, and N. S. Febrianta, "Desain Antarmuka Pengguna Aplikasi Telemedicine," *Jurnal Manajemen Informasi Kesehatan Indonesia*, vol. 12, no. 1, pp. 85–89, 2024, doi: 10.33560/jmiki.v12i1.659.
- [22] S. Darmiani, B. Y. Pratama, B. Islamy, and T. A. Hidayat, "Tantangan Integrasi Rekam Medis Elektronik dengan Sistem Manajemen Rumah Sakit: Dampak pada Keamanan Data dan Efisiensi Biaya Operasional," *Jurnal Sosial dan Sains (SOSAINS)*, vol. 4, pp. 1107–1116, Nov. 2024.
- [23] S. Handayani and A. Budiman, "Tinjauan Faktor Keamanan dan Kerahasiaan Rekam Medis di Rumah Sakit TK. III Dr. R. Soeharsono Banjarmasin," *Jurnal Manajemen Informasi Kesehatan Indonesia*, vol. 12, no. 1, pp. 57–64, 2024, doi: 10.33560/jmiki.v12i1.641.
- [24] S. Jaya Bahwiyanti, "Jurnal Ilmiah Ekonomi Bisnis," *Jurnal Ilmiah Ekonomi Bisnis (JIEB)*, vol. 5, pp. 1–12, Nov. 2020.
- [25] Sugiyono. (2022). *Metode penelitian kualitatif*. Alfabeta.
- [26] V. Febriyana and A. Ichwani, "Keamanan Data Rekam Medis Elektronik Menggunakan Teknik Kriptografi: Literature Review," *Ilmu Komputer Unila Publishing Network*, vol. 12, no. 2, pp. 165–175, 2023.
- [27] World Health Organization. (2021). *Global Strategy on Digital Health 2020–2025*. Geneva: World Health Organization.
- [28] Yusuf, A. M. (2017). *Metode penelitian: Kuantitatif, kualitatif, dan penelitian gabungan*. Kencana.