Empiricism Journal
https://journal-center.litpam.com/index.php/empiricism
email: empiric.journal@gmail.com

Vol. 7, No 3, Sep. 2026
e-ISSN: 2745-7613
pp. 2651-2663

Audit Sistem Informasi Rekam Medis Elektronik (RME) Berbasis Kriteria ISO/IEC 27001:2022 di UPT Puskesmas Cibiuk

Nur Rizal Fahmana[1], Purnomo Sidiq[2], Dinar Rahayu[3]
[123]Program Studi Sistem Informasi, Fakultas Ilmu Terapan dan Sains, Institut Pendidikan Indonesia (IPI) Garut, Indonesia
Email Korespondensi: nzfahmana@gmail.com

Abstrak

Digitalisasi layanan fasilitas kesehatan menjadi tuntutan yang tidak dapat dihindari pada era abad ke-21, termasuk pada layanan Rekam Medis Elektronik (RME) di lingkungan Fasilitas Pelayanan Kesehatan Tingkat Pertama (FKTP). Urgensi audit keamanan RME di FKTP semakin meningkat seiring dengan maraknya insiden kebocoran data kesehatan dan belum meratanya penerapan standar keamanan informasi di tingkat primer. Penelitian ini bertujuan untuk mengaudit keamanan sistem informasi RME pada UPT Puskesmas Cibiuk guna mengevaluasi proses tata kelola perlindungan privasi data pasien yang masih berjalan tanpa standar keamanan baku dan rentan terhadap kebocoran akses. Metode yang digunakan adalah Audit Sistem Informasi melalui pendekatan Gap Analysis (Analisis Kesenjangan), yang dijalankan dengan mengevaluasi 8 kontrol pada Annex A.6 People Controls dan 23 kontrol internal pada Annex A.8 Technological Controls ISO/IEC 27001:2022. Subjek penelitian adalah pengelola IT dan tenaga medis pengguna sistem di UPT Puskesmas Cibiuk, sedangkan objek penelitian adalah sistem RME yang saat ini digunakan secara aktif di poli pelayanan. Hasil penelitian menunjukkan bahwa tingkat kematangan (maturity level) keamanan sistem berada pada rata-rata 2.30 (Repeatable) dengan persentase kesesuaian sebesar 47,09%. Temuan risiko tertinggi ditemukan pada kontrol backup yang belum diuji restore dengan risk score 20 (Sangat Tinggi). Celah keamanan paling signifikan ditemukan pada praktik berbagi kata sandi (password sharing) antar perawat dan ketiadaan enkripsi pada proses pencadangan (backup) data. Implementasi audit terbukti efektif memetakan kerentanan sistematis pada operasional puskesmas. Penelitian ini menyimpulkan bahwa kerangka kerja ISO/IEC 27001:2022 sangat relevan diterapkan pada evaluasi sistem informasi berskala layanan kesehatan primer karena ketatnya standar yang mengakomodasi perlindungan data medis.

Kata kunci: Audit Sistem Informasi; RME; Keamanan Informasi; ISO/IEC 27001:2022.

Audit of Electronic Medical Record (EMR) Information System Based on ISO/IEC 27001:2022 Criteria at UPT Puskesmas Cibiuk

Abstract

The digitalization of healthcare facilities has become an unavoidable demand in the 21st century, including Electronic Medical Record (EMR) services in Primary Healthcare Facilities. The urgency of auditing EMR security in primary healthcare facilities is increasing along with the rise in health data breach incidents and the uneven implementation of information security standards at the primary level. This study aims to audit the security of the EMR information system at UPT Puskesmas Cibiuk to evaluate the governance of patient data privacy protection, which is currently running without standard security protocols and is vulnerable to access breaches. The method used is Information Systems Audit through a Gap Analysis approach, conducted by evaluating 8 controls in Annex A.6 People Controls and 23 internal controls in Annex A.8 Technological Controls of ISO/IEC 27001:2022. The research subjects were IT administrators and medical personnel using the system at UPT Puskesmas Cibiuk, while the object of research was the EMR system currently actively used in outpatient clinics. The results showed that the system's security maturity level is at an average of 2.30 (Repeatable) with a compliance percentage of 47.09%. The highest risk finding was found in the backup control that had not been restore-tested, with a risk score of 20 (Very High). The most significant security vulnerabilities were found in the practice of password sharing among nurses and the lack of encryption in the data backup process. The implementation of the audit proved effective in mapping systematic vulnerabilities in the community health center's operations. This study concludes that the ISO/IEC 27001:2022 framework is highly relevant for evaluating information systems at the primary healthcare level due to its strict standards accommodating medical data protection.

Keywords: *Information System Audit; EMR; Information Security; ISO/IEC 27001:2022; UPT Puskesmas Cibiuk*

How to Cite: Fahmana, N. R. ., Purnomo, & Rahayu, D. . (2026). Audit Sistem Informasi Rekam Medis Elektronik (RME) Berbasis Kriteria ISO/IEC 27001:2022 di UPT Puskesmas Cibiuk. *Empiricism Journal*, *7*(3), 2651-2663. https://doi.org/10.36312/ej.v7i3.6542

https://doi.org/10.36312/ej.v7i3.6542

PENDAHULUAN

Transformasi digital pada sektor kesehatan telah mendorong fasilitas pelayanan kesehatan untuk menggunakan Rekam Medis Elektronik (RME) dalam proses pelayanan (Asih et al., 2024; Pramesti et al., 2024). RME memberikan manfaat berupa kemudahan pencatatan, penyimpanan, pencarian, dan pertukaran informasi kesehatan (Ikawati et al., 2025). Namun, perubahan dari rekam medis berbasis kertas menuju sistem elektronik juga meningkatkan ketergantungan terhadap aplikasi, perangkat, jaringan, basis data, serta sumber daya manusia yang mengoperasikan sistem (Igayanti et al., 2026; Setyaningrum & Ricky, 2025).

Keamanan informasi RME menjadi isu penting karena informasi kesehatan berkaitan langsung dengan privasi pasien. Konsep CIA Triad (Confidentiality, Integrity, Availability) menjadi landasan utama dalam menjaga keamanan informasi di lingkungan kesehatan (Whitman & Mattord, 2022). Gangguan terhadap kerahasiaan, integritas, maupun ketersediaan informasi dapat menimbulkan dampak terhadap pasien dan keberlangsungan pelayanan (Simanullang et al., 2026; Rani & Widyaningrum, 2025). Risiko tersebut dapat muncul akibat kesalahan manusia, penggunaan akun yang tidak sesuai, lemahnya autentikasi, malware, kerentanan teknis, kehilangan perangkat, kegagalan backup, maupun gangguan jaringan (Soraya et al., 2025).

ISO/IEC 27001:2022 menyediakan kerangka sistem manajemen keamanan informasi dan kontrol yang dapat digunakan organisasi untuk mengelola risiko keamanan informasi (ISO, 2022a). Standar ini merupakan pembaruan dari ISO/IEC 27001:2013 dengan perubahan signifikan pada struktur Annex A yang kini mengelompokkan kontrol ke dalam empat klaster: organizational, people, physical, dan technological controls (ISO, 2022b). Annex A pada edisi 2022 terdiri dari empat kelompok kontrol, yaitu organizational controls, people controls, physical controls, dan technological controls. Penelitian ini secara khusus membatasi ruang lingkup pada Annex A.6 People Controls dan kontrol internal Annex A.8 Technological Controls agar audit lebih terfokus pada faktor sumber daya manusia serta pengendalian teknologi yang mendukung RME (Fathurohman & Witjaksono, 2020).

Di Indonesia, implementasi RME diatur melalui Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis yang mewajibkan fasilitas pelayanan kesehatan untuk menyelenggarakan rekam medis elektronik secara bertahap (Kemenkes RI, 2022). Regulasi ini sejalan dengan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang memberikan perlindungan hukum terhadap data kesehatan sebagai data pribadi yang sensitif (Republik Indonesia, 2022). Namun, implementasi RME di fasilitas kesehatan tingkat pertama (FKTP) masih menghadapi berbagai tantangan, terutama dari sisi infrastruktur teknologi, sumber daya manusia, dan kepatuhan terhadap standar keamanan informasi (Arif et al., 2026).

Annex A.6 terdiri atas delapan kontrol yang berkaitan dengan screening, ketentuan kerja, awareness dan pelatihan keamanan informasi, proses disipliner, tanggung jawab setelah terminasi atau perubahan pekerjaan, confidentiality/non-disclosure agreement, remote working, serta pelaporan kejadian keamanan informasi (ISO, 2022b). Kontrol tersebut relevan karena pengguna RME memiliki peran langsung dalam menjaga keamanan informasi pasien (Ikawati & Ansyori, 2025).

Annex A.8 terdiri atas tiga puluh empat kontrol teknologi yang mencakup perangkat endpoint, privileged access, pembatasan akses informasi, source code, autentikasi, capacity management, malware protection, vulnerability management, konfigurasi, information deletion, data masking, data leakage prevention, backup, redundancy, logging, monitoring, time synchronization, utility programs, privileged installation, network security, network segregation, web filtering, cryptography, secure development, application security, secure architecture, secure coding, security testing, outsourced development, separation of environments, change management, test information, dan protection during audit testing (ISO, 2022b). Kelompok kontrol tersebut memungkinkan audit dilakukan dari sisi teknologi secara lebih komprehensif (Rumetna et al., 2022).

Pada tingkat fasilitas pelayanan kesehatan primer, audit keamanan RME diperlukan agar pengelola dapat mengetahui kondisi kontrol yang sudah diterapkan, kontrol yang belum

tersedia, dan kontrol yang telah tersedia tetapi belum efektif (Mariani, 2025). Hasil audit dapat menjadi dasar penyusunan prioritas perbaikan berdasarkan tingkat risiko.

Penelitian terdahulu menunjukkan bahwa keamanan RME masih menghadapi berbagai persoalan. Studi pada RS Panti Nugroho menunjukkan pentingnya pengelolaan user ID, password, dan hak akses (We'e et al., 2023). Penelitian di RSUD Klungkung menemukan persoalan terkait kedisiplinan pengguna serta pengaturan username dan password (Mariani, 2025). Penelitian lain menggunakan gap analysis berbasis ISO 27001 untuk mengevaluasi keamanan informasi RME (Arif et al., 2026; Rani & Widyaningrum, 2025). Temuan tersebut menunjukkan bahwa pengamanan RME perlu memperhatikan kombinasi antara manusia dan teknologi (Ardianto et al., 2024).

Namun, masih terdapat kesenjangan penelitian (research gap) dalam hal audit keamanan RME di tingkat fasilitas kesehatan primer (FKTP) seperti Puskesmas. Sebagian besar penelitian sebelumnya berfokus pada rumah sakit yang memiliki sumber daya dan infrastruktur lebih memadai. Penelitian di UPT Puskesmas Cibiuk menjadi penting karena representatif terhadap kondisi FKTP di Indonesia yang memiliki keterbatasan sumber daya manusia, anggaran, dan infrastruktur teknologi, namun tetap dituntut untuk melindungi data pasien sesuai regulasi. Penelitian ini berbeda dari penelitian sebelumnya karena secara spesifik mengaudit aspek people dan technological controls dengan pendekatan gap analysis yang terukur, serta memberikan rekomendasi praktis yang sesuai dengan kapasitas FKTP.

METODE

Penelitian ini menggunakan pendekatan deskriptif dengan metode gap analysis untuk mengevaluasi tingkat kematangan keamanan informasi pada sistem Rekam Medis Elektronik (RME) di UPT Puskesmas Cibiuk berdasarkan kriteria ISO/IEC 27001:2022. Metode gap analysis dipilih karena mampu membandingkan kondisi aktual penerapan kontrol dengan kondisi ideal yang diharapkan, sehingga kesenjangan (gap) dapat diidentifikasi secara sistematis untuk menentukan prioritas perbaikan (Bahaudin & Rizqi, 2024; Weber, 2010; Hall, 2015). Pendekatan deskriptif digunakan untuk menggambarkan secara mendalam kondisi objektif setiap kontrol keamanan informasi berdasarkan bukti-bukti yang ditemukan di lapangan. Ruang lingkup audit dibatasi pada kontrol yang berada dalam kewenangan internal puskesmas, yaitu Annex A.6 People Controls dan kontrol internal yang relevan pada Annex A.8 Technological Controls, sedangkan aspek pengembangan aplikasi, source code, dan pengendalian internal pihak ketiga tidak termasuk dalam objek audit karena aplikasi RME diperoleh dari pihak luar. Data penelitian diperoleh melalui observasi, wawancara, telaah dokumen, dan pemeriksaan bukti pengendalian keamanan informasi. Penilaian setiap kontrol menggunakan skala kematangan (maturity level) 1--5, yaitu Initial, Repeatable, Defined, Managed, dan Optimized, yang digunakan untuk menggambarkan tingkat penerapan, dokumentasi, evaluasi, dan perbaikan berkelanjutan terhadap masing-masing kontrol (Romney & Steinbart, 2018).

Tabel 1. Instrumen Annex A.6 People Control

Kontrol	Nama Kontrol	Kriteria Audit	Bukti yang Diperiksa
A.6.1	Screening	Pemeriksaan latar belakang personel sesuai hukum, regulasi, dan etika serta kebutuhan organisasi.	Dokumen screening/rekrutmen
A.6.2	Terms and Conditions of Employment	Ketentuan kerja memuat tanggung jawab keamanan informasi.	Kontrak/SK/ketentuan kerja
A.6.3	Information Security Awareness, Education and Training	Pengguna memperoleh awareness, pendidikan, dan pelatihan keamanan informasi.	Materi, daftar hadir, evaluasi
A.6.4	Disciplinary Process	Tersedia proses disipliner	SOP/tata tertib/bukti

Kontrol	Nama Kontrol	Kriteria Audit	Bukti yang Diperiksa
		terhadap pelanggaran keamanan informasi.	tindakan
A.6.5	Responsibilities After Termination or Change of Employment	Tanggung jawab keamanan setelah terminasi atau perubahan pekerjaan ditetapkan dan dikomunikasikan.	SOP/offboarding/SK
A.6.6	Confidentiality or Non-Disclosure Agreements	Kewajiban kerahasiaan atau NDA diterapkan sesuai kebutuhan.	NDA/perjanjian
A.6.7	Remote Working	Keamanan informasi saat bekerja jarak jauh dikelola sesuai risiko.	Kebijakan remote working
A.6.8	Information Security Event Reporting	Pengguna memiliki mekanisme untuk melaporkan kejadian keamanan informasi.	SOP/form/log pelaporan

Tabel 2. Instrumen Annex A.8 Technological Controls

Kontrol	Nama Kontrol	Kriteria Audit	Bukti yang Diperiksa
A.8.1	User endpoint devices	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.2	Privileged access rights	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.3	Information access restriction	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.5	Secure authentication	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.6	Capacity management	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.7	Protection against malware	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.8	Management of technical vulnerabilities	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.9	Configuration	Penerapan kontrol pada perangkat,	Observasi, SOP, daftar

Kontrol	Nama Kontrol	Kriteria Audit	Bukti yang Diperiksa
	management	akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.10	Information deletion	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.11	Data masking	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.12	Data leakage prevention	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.13	Information backup	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.14	Redundancy of information processing facilities	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.15	Logging	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.16	Monitoring activities	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.17	Clock synchronization	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.18	Use of privileged utility programs	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.19	Installation of software on operational systems	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.20	Networks	Penerapan kontrol pada perangkat,	Observasi, SOP, daftar

Kontrol	Nama Kontrol	Kriteria Audit	Bukti yang Diperiksa
	security	akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.21	Security of network services	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.22	Segregation of networks	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.23	Web filtering	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.24	Use of cryptography	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.
A.8.32	Change management	Penerapan kontrol pada perangkat, akun, jaringan, proses, dan teknologi yang berada dalam kewenangan internal UPT Puskesmas Cibiuk.	Observasi, SOP, daftar akun, konfigurasi, log, backup, perangkat, jaringan, dan bukti operasional.

Tabel 3. Tingkat Kematangan

Skor	Tingkat Kematangan	Deskripsi dan Syarat Pemenuhan	Skor
1	Initial (Sangat Kurang)	Praktik keamanan tidak diterapkan, atau dilakukan acak/ad-hoc dan tidak konsisten. Keamanan bergantung pada inisiatif individu.	1
2	Repeatable (Kurang)	Praktik keamanan sudah dilakukan rutin sebagai kebiasaan, tetapi belum memiliki dokumen resmi (SOP/SK).	2
3	Defined (Cukup / Sesuai)	Praktik keamanan telah dibakukan, didokumentasikan dalam SOP/SK resmi, dan dikomunikasikan kepada pegawai.	3
4	Managed (Baik)	Terdapat SOP tertulis dan manajemen melakukan evaluasi/audit internal secara berkala.	4
5	Optimized (Sangat Baik)	Praktik menjadi budaya organisasi, dilakukan continuous improvement, dan didukung otomatisasi teknologi.	5

Analisis Risiko

Setelah tingkat kematangan dan kesenjangan setiap kontrol diidentifikasi, dilakukan analisis risiko untuk menentukan prioritas penanganan. Penilaian risiko menggunakan dua parameter, yaitu kemungkinan terjadinya risiko (likelihood) dan dampak risiko (impact), dengan rentang nilai 1--5. Risk Score dihitung menggunakan rumus Risk Score = Likelihood × Impact. Nilai yang diperoleh kemudian dipetakan ke dalam tingkat risiko dan digunakan untuk menentukan urutan prioritas tindakan perbaikan.

Tabel 4. Matrix Penilaian Risiko

Likelihood \ Impact	1	2	3	4	5
5 – Almost Certain	5	10	15	20	25
4 – Likely	4	8	12	16	20
3 – Possible	3	6	9	12	15
2 – Unlikely	2	4	6	8	10
1 – Rare	1	2	3	4	5

Kriteria tingkat risiko yang digunakan dalam penelitian ini adalah 1--4 = Rendah, 5--9 = Sedang, 10--16 = Tinggi, dan 17--25 = Sangat Tinggi. Kategori tersebut digunakan sebagai dasar penentuan prioritas tindakan korektif. Prioritas 1 diberikan kepada temuan dengan tingkat risiko paling tinggi.

Sampel/Subjek Penelitian

Subjek penelitian adalah pihak-pihak di UPT Puskesmas Cibiuk yang terlibat langsung dalam penggunaan, pengelolaan, dan pengawasan sistem Rekam Medis Elektronik, yang dipilih menggunakan teknik purposive sampling. Informan penelitian berjumlah 5 (lima) orang, meliputi petugas atau penanggung jawab rekam medis, tenaga kesehatan yang menggunakan RME dalam pelayanan, petugas administrasi atau pendaftaran, serta petugas yang memiliki tanggung jawab terhadap pengelolaan sistem atau teknologi informasi di lingkungan puskesmas. Pemilihan informan didasarkan pada pertimbangan bahwa mereka memahami proses penggunaan RME, pengelolaan akun dan hak akses, penerapan prosedur keamanan, serta pengendalian teknologi yang digunakan dalam kegiatan pelayanan. Jumlah informan disesuaikan dengan kondisi dan ketersediaan pihak yang terlibat langsung di UPT Puskesmas Cibiuk.

Instrumen dan Prosedur Penelitian

Instrumen penelitian yang digunakan meliputi pedoman wawancara semi-terstruktur yang memuat pertanyaan-pertanyaan terkait penerapan setiap kontrol Annex A.6 dan A.8, lembar observasi untuk memeriksa langsung kondisi fisik dan teknologi, lembar telaah dokumen untuk mengevaluasi ketersediaan dan kelengkapan dokumen kebijakan dan prosedur, serta checklist audit berdasarkan kontrol ISO/IEC 27001:2022 yang menjadi ruang lingkup penelitian. Kisi-kisi pedoman wawancara disusun berdasarkan setiap kontrol yang diaudit, dengan indikator pertanyaan yang mengacu pada kriteria audit dan bukti yang diperiksa. Instrumen audit mencakup delapan kontrol pada Annex A.6 People Controls dan kontrol pada Annex A.8 Technological Controls yang relevan dengan kewenangan internal UPT Puskesmas Cibiuk. Prosedur pengumpulan data dilaksanakan secara kronologis melalui beberapa tahap: (1) Tahap Persiapan (1 minggu): penentuan ruang lingkup audit, penyusunan instrumen, dan koordinasi dengan pihak puskesmas; (2) Tahap Pengumpulan Data (2 minggu): pelaksanaan wawancara dengan masing-masing informan selama 30-45 menit, observasi langsung terhadap sistem dan lingkungan kerja, serta telaah dokumen; (3) Tahap Pemeriksaan Bukti (1 minggu): verifikasi dan triangulasi data dari berbagai sumber; dan (4) Tahap Analisis dan Pelaporan (1 minggu): penilaian maturity level, identifikasi gap, analisis risiko, dan penyusunan rekomendasi. Pengumpulan data dilakukan melalui wawancara dengan informan untuk memperoleh informasi mengenai penerapan kebijakan dan praktik keamanan informasi, observasi terhadap penggunaan RME, perangkat, akun, jaringan, serta lingkungan operasional, dan telaah terhadap dokumen seperti SOP, SK, bukti pelatihan, daftar pengguna, bukti backup, log aktivitas, serta dokumen pengendalian lainnya. Setiap kontrol kemudian dinilai menggunakan maturity level 1--5 berdasarkan bukti yang ditemukan, kemudian dicatat kondisi penerapan, kesenjangan (gap), risiko, dan rekomendasi perbaikan.

Analisis Data

Data hasil audit dianalisis menggunakan teknik analisis deskriptif dengan menghitung tingkat kematangan setiap kontrol berdasarkan skor maturity level 1--5, kemudian dilakukan rekapitulasi untuk kelompok Annex A.6 dan kontrol internal Annex A.8. Nilai rata-rata tingkat kematangan dihitung dengan membandingkan total skor yang diperoleh dengan jumlah kontrol yang dinilai, sedangkan persentase tingkat kesesuaian dihitung menggunakan rumus jumlah skor yang diperoleh dibagi skor maksimum kemudian dikalikan 100%. Hasil penilaian

selanjutnya dianalisis untuk mengidentifikasi kesenjangan antara kondisi aktual dan kondisi yang diharapkan berdasarkan kriteria kontrol yang digunakan. Temuan yang memiliki dampak dan kemungkinan kejadian lebih tinggi diprioritaskan melalui analisis risiko untuk menentukan rekomendasi perbaikan. Data hasil wawancara dan observasi digunakan sebagai pendukung interpretasi terhadap hasil penilaian kuantitatif sehingga diperoleh gambaran menyeluruh mengenai tingkat kematangan keamanan informasi pada pengelolaan RME di UPT Puskesmas Cibiuk.

HASIL DAN PEMBAHASAN

Profil UPT Puskesmas Cibiuk

UPT Puskesmas Cibiuk merupakan fasilitas kesehatan tingkat pertama yang terletak di Kabupaten Garut, Jawa Barat. Puskesmas ini memiliki jumlah pegawai sebanyak 32 orang yang terdiri dari tenaga medis, paramedis, dan tenaga administrasi. Rata-rata jumlah pasien yang dilayani mencapai 60-80 pasien per hari. Sistem RME yang digunakan merupakan aplikasi berbasis web yang dikembangkan oleh pihak ketiga dan telah beroperasi sejak tahun 2021. Sistem ini digunakan untuk pencatatan medis, pendaftaran pasien, dan pelaporan.

Hasil audit keamanan informasi pada sistem Rekam Medis Elektronik (RME) di UPT Puskesmas Cibiuk diperoleh melalui proses observasi, wawancara, telaah dokumen, dan pemeriksaan bukti pengendalian berdasarkan kriteria ISO/IEC 27001:2022 yang telah ditetapkan dalam penelitian. Penilaian dilakukan terhadap kontrol Annex A.6 People Controls dan kontrol internal yang relevan pada Annex A.8 Technological Controls dengan menggunakan skala kematangan (maturity level) 1--5, yaitu Initial, Repeatable, Defined, Managed, dan Optimized. Setiap kontrol dinilai berdasarkan kondisi penerapan dan bukti yang ditemukan di lapangan, kemudian dilakukan rekapitulasi untuk mengetahui tingkat kematangan pada masing-masing kelompok kontrol. Hasil penilaian tersebut selanjutnya disajikan pada tabel berikut.

Tabel 5. Hasil Instrumen Annex A.6 People Controls

Kontrol	Nama	Level	Bukti/Temuan	Gap	Rekomendasi
A.6.1	Screening	3	Proses screening dilakukan saat rekrutmen, tetapi bukti belum seragam.	Gap: checklist screening belum baku.	Standarkan checklist screening.
A.6.2	Terms and Conditions of Employment	3	Ketentuan kerja memuat kewajiban menjaga kerahasiaan.	Gap: klausul keamanan belum seragam.	Standarkan klausul keamanan informasi.
A.6.3	Awareness, Education and Training	2	Pengarahan keamanan diberikan secara informal.	Gap: belum ada program pelatihan berkala terdokumentasi.	Buat program awareness tahunan.
A.6.4	Disciplinary Process	2	Pelanggaran ditangani melalui tata tertib umum.	Gap: prosedur khusus keamanan belum ada.	Integrasikan keamanan ke proses disipliner.
A.6.5	Responsibilities After Termination/Change	3	Pencabutan/perubahan akses dilakukan setelah pemberitahuan.	Gap: checklist offboarding belum konsisten.	Buat checklist offboarding.
A.6.6	Confidentiality / NDA	2	Pegawai memahami kerahasiaan melalui ketentuan umum.	Gap: pernyataan kerahasiaan belum seragam.	Standarkan pernyataan kerahasiaan.

Kontrol	Nama	Level	Bukti/Temuan	Gap	Rekomendasi
A.6.7	Remote Working	1	Tidak ditemukan kebijakan remote working khusus RME.	Gap: belum ada aturan formal.	Tetapkan kebijakan remote access.
A.6.8	Information Security Event Reporting	2	Pelaporan dilakukan langsung kepada penanggung jawab.	Gap: mekanisme belum terdokumentasi.	Buat SOP/form pelaporan insiden.

Tabel 6. Hasil Instrumen Annex A.8 Technological Controls Internal

Kontrol	Nama	Level	Bukti/Temuan	Gap	Rekomendasi
A.8.1	User endpoint devices	3	Endpoint memiliki proteksi dasar.	Inventaris/baseline belum lengkap.	Lengkapi inventaris dan baseline.
A.8.2	Privileged access rights	3	Akun admin dibatasi petugas tertentu.	Review hak akses belum berkala.	Review hak akses berkala.
A.8.3	Information access restriction	3	Hak akses berdasarkan fungsi.	Matriks akses belum lengkap.	Buat matriks role/access.
A.8.5	Secure authentication	3	Username/password diterapkan.	Review autentikasi belum berkala.	Tetapkan standar autentikasi.
A.8.6	Capacity management	3	Kapasitas dipantau operasional.	Threshold belum terdokumentasi.	Tetapkan indikator kapasitas.
A.8.7	Protection against malware	3	Proteksi malware tersedia pada endpoint.	Monitoring belum seragam.	Standarkan proteksi endpoint.
A.8.8	Technical vulnerabilities	2	Kerentanan ditangani bila ditemukan.	Belum ada vulnerability management formal.	Buat pencatatan kerentanan.
A.8.9	Configuration management	2	Konfigurasi dilakukan petugas/vendor.	Baseline konfigurasi belum terdokumentasi.	Dokumentasikan baseline.
A.8.10	Information deletion	2	Penghapusan dilakukan sesuai kebutuhan.	Prosedur belum terdokumentasi.	Buat prosedur penghapusan.
A.8.11	Data masking	1	Belum ditemukan masking khusus.	Belum diterapkan.	Evaluasi kebutuhan masking.
A.8.12	Data leakage prevention	1	Belum ada DLP khusus.	Belum diterapkan.	Evaluasi kebutuhan DLP.
A.8.13	Information backup	3	Backup tersedia.	Uji restore belum terdokumentasi lengkap.	Lakukan restore test.
A.8.14	Redundancy	2	Ketersediaan bergantung infrastruktur tersedia.	Redundancy belum terverifikasi.	Identifikasi single point of failure.
A.8.15	Logging	3	Log aktivitas tertentu tersedia.	Review log belum berkala.	Tetapkan prosedur review log.

Kontrol	Nama	Level	Bukti/Temuan	Gap	Rekomendasi
A.8.16	Monitoring activities	2	Monitoring dilakukan saat gangguan.	Monitoring keamanan belum terstruktur.	Tetapkan monitoring berkala.
A.8.17	Clock synchronization	3	Sinkronisasi waktu tersedia.	Verifikasi belum terdokumentasi.	Verifikasi berkala.
A.8.18	Privileged utility programs	2	Utility administratif dibatasi.	Otorisasi belum terdokumentasi.	Dokumentasikan otorisasi.
A.8.19	Software installation	2	Instalasi software dibatasi.	Pencatatan belum formal.	Buat prosedur instalasi.
A.8.20	Networks security	3	Jaringan internal memiliki kontrol dasar.	Dokumentasi baseline belum lengkap.	Dokumentasikan baseline jaringan.
A.8.21	Security of network services	3	Layanan jaringan dikelola operasional.	Standar keamanan belum lengkap.	Dokumentasikan standar layanan.
A.8.22	Segregation of networks	2	Segmentasi belum menyeluruh.	Pemisahan jaringan belum optimal.	Evaluasi segmentasi/VLAN.
A.8.23	Web filtering	2	Web filtering khusus RME belum lengkap.	Masih terdapat data yang belum terfilter.	Evaluasi web filtering.
A.8.24	Use of cryptography	2	Kriptografi mengikuti fitur aplikasi/vendor.	Standar internal belum terdokumentasi.	Tetapkan standar kriptografi.

Tabel 7. Hasil Instrumen Annex A.6 dan A.8

Kelompok	Jumlah Kontrol	Skor Maksimum	Skor	Persentase	Interpretasi
A.6 People Controls	8	40	18	45.00%	Repeatable / Kurang
A.8 Technological Controls	23	115	55	47.82%	Repeatable / Kurang
Total	31	155	73	47.09%	Repeatable / Kurang

Interpretasi terhadap hasil audit menunjukkan bahwa People Controls memperoleh rata-rata kematangan 2.25, yang berarti praktik keamanan sudah dilakukan secara rutin tetapi belum didokumentasikan secara formal. Temuan paling lemah pada remote working (Level 1) mengindikasikan bahwa puskesmas belum memiliki kebijakan formal untuk bekerja dari jarak jauh, yang sangat berisiko jika terjadi situasi darurat atau kebutuhan akses dari luar kantor. Sementara itu, screening, ketentuan kerja, dan tanggung jawab setelah perubahan pekerjaan berada pada Level 3, menunjukkan bahwa prosedur telah dijalankan tetapi belum terstandarisasi secara penuh.

Technological Controls memperoleh rata-rata kematangan 2.35, dengan gap utama pada data masking, data leakage prevention, web filtering, vulnerability management, monitoring, dan segmentasi jaringan. Temuan ini menunjukkan bahwa perlindungan data terhadap kebocoran dan serangan siber masih lemah. Praktik password sharing yang ditemukan di lapangan memperparah kondisi ini karena akun yang digunakan bersama sulit dilacak dan berpotensi disalahgunakan. Ketiadaan enkripsi pada backup juga menjadi temuan kritis karena jika media backup hilang, seluruh data pasien dapat terekspos tanpa perlindungan.

Perbandingan dengan penelitian terdahulu menunjukkan bahwa temuan serupa juga ditemukan di RS Panti Nugroho (We'e et al., 2023) dan RSUD Klungkung (Mariani, 2025),

terutama dalam hal pengelolaan akun dan hak akses. Namun, penelitian ini menemukan kelemahan yang lebih spesifik pada aspek remote working dan segmentasi jaringan yang belum banyak diungkap dalam penelitian sebelumnya di FKTP. Hal ini menunjukkan bahwa FKTP memiliki karakteristik tantangan yang berbeda dibandingkan rumah sakit, terutama dari sisi sumber daya dan infrastruktur.

Analisis risiko lebih mendalam untuk setiap temuan menunjukkan bahwa backup yang belum diuji restore dapat menyebabkan kegagalan pemulihan data pasca-insiden, yang berpotensi menghentikan operasional puskesmas selama berhari-hari. Skenario dampak ini dapat mengakibatkan penurunan kepercayaan pasien dan sanksi regulasi. Demikian pula, password sharing dapat menyebabkan akses tidak sah yang sulit dilacak, sehingga jika terjadi kebocoran data, sulit untuk mengidentifikasi pelaku dan mengambil tindakan korektif.

Risk Matrix

Berdasarkan hasil identifikasi kesenjangan pada masing-masing kontrol keamanan informasi, selanjutnya dilakukan analisis risiko untuk menentukan tingkat risiko dan prioritas penanganan terhadap temuan yang diperoleh. Penilaian risiko dilakukan dengan mempertimbangkan kemungkinan terjadinya risiko (likelihood) dan besarnya dampak (impact) terhadap keamanan serta keberlangsungan sistem Rekam Medis Elektronik (RME). Nilai risiko diperoleh dari perkalian antara likelihood dan impact, kemudian digunakan untuk menentukan tingkat risiko dan urutan prioritas tindakan perbaikan. Hasil analisis risiko pada temuan yang memiliki tingkat risiko paling signifikan disajikan pada Tabel.

Tabel 8. Risk Matrix

Temuan	Likelihood	Impact	Risk Score	Tingkat Risiko	Prioritas	Tindakan
Backup belum diuji restore	4	5	20	Sangat Tinggi	1	Lakukan restore test dan dokumentasikan.
Review hak akses belum berkala	4	4	16	Tinggi	2	Review seluruh akun dan hak akses.
Pelaporan insiden belum terdokumentasi	4	4	16	Tinggi	3	Buat SOP dan formulir insiden.
Training keamanan belum berkala	3	4	12	Tinggi	4	Jadwalkan awareness periodik.
Segmentasi jaringan belum optimal	3	4	12	Tinggi	5	Evaluasi segmentasi jaringan.

Berdasarkan Tabel, temuan dengan nilai risiko tertinggi adalah kondisi backup yang belum diuji restore, dengan nilai risk score sebesar 20 yang termasuk dalam kategori sangat tinggi. Jika terjadi kegagalan sistem atau serangan ransomware, puskesmas tidak memiliki jaminan bahwa data pasien dapat dipulihkan, yang dapat menghentikan pelayanan kesehatan dan meni mbulkan kerugian besar. Kondisi tersebut menjadi prioritas utama karena kegagalan proses pemulihan data dapat berdampak langsung terhadap ketersediaan informasi RME ketika terjadi gangguan atau kehilangan data. Temuan berikutnya adalah review hak akses dan mekanisme pelaporan insiden yang masing-masing memperoleh nilai risiko 16 dan termasuk kategori tinggi. Risiko yang terkait dengan hak akses yang tidak ditinjau secara berkala dapat menyebabkan akun yang tidak aktif tetap memiliki akses ke sistem, serta pengguna memiliki hak akses yang tidak sesuai dengan fungsi pekerjaannya. Kondisi tersebut menunjukkan bahwa pengendalian akses dan kemampuan organisasi dalam mendeteksi serta merespons kejadian keamanan masih memerlukan penguatan. Sementara itu, belum optimalnya pelatihan keamanan serta segmentasi jaringan memperoleh nilai risiko 12 dan tetap termasuk kategori tinggi, sehingga kedua aspek tersebut perlu dimasukkan dalam rencana tindak lanjut perbaikan keamanan informasi.

KESIMPULAN

Berdasarkan hasil audit sistem informasi Rekam Medis Elektronik (RME) di UPT Puskesmas Cibiuk menggunakan kriteria ISO/IEC 27001:2022 pada Annex A.6 People Controls dan kontrol internal yang relevan pada Annex A.8 Technological Controls, penelitian ini menyimpulkan bahwa tingkat kematangan keamanan informasi RME secara keseluruhan berada pada level 2.30 (Repeatable) dengan persentase kesesuaian 47,09%. Hal ini menunjukkan bahwa penerapan kontrol keamanan informasi masih berada pada tahap kebiasaan rutin tanpa dokumentasi formal dan evaluasi berkala, sehingga diperlukan peningkatan signifikan untuk mencapai level yang lebih baik (Defined/Level 3). Penerapan metode gap analysis terbukti efektif dalam memetakan kerentanan sistem secara sistematis, mengidentifikasi kesenjangan antara kondisi aktual dan ideal, serta memberikan dasar untuk menentukan prioritas perbaikan berdasarkan tingkat risiko.

Penelitian ini memiliki beberapa keterbatasan, antara lain: (1) ruang lingkup audit hanya mencakup kontrol internal Annex A.6 dan A.8 yang menjadi kewenangan puskesmas, sehingga tidak mencakup aspek pengembangan aplikasi dan pengendalian pihak ketiga; (2) jumlah informan terbatas pada 5 orang yang terlibat langsung dengan sistem RME; dan (3) penelitian dilakukan dalam periode waktu terbatas sehingga tidak dapat menangkap dinamika perubahan keamanan informasi dalam jangka panjang. Meskipun demikian, hasil penelitian ini memberikan gambaran yang cukup komprehensif mengenai kondisi keamanan RME di FKTP dan rekomendasi perbaikan yang dapat diimplementasikan secara bertahap.

REKOMENDASI

Berdasarkan hasil audit dan analisis risiko, UPT Puskesmas Cibiuk disarankan untuk memprioritaskan perbaikan pada pengelolaan backup dan recovery, hak akses pengguna, pelaporan insiden, pelatihan keamanan informasi, serta keamanan jaringan dan monitoring. Selain itu, dokumentasi SOP, evaluasi berkala, dan pengendalian terhadap pengguna perlu diperkuat agar penerapan kontrol tidak hanya berjalan sebagai kebiasaan, tetapi dapat meningkat menuju tingkat Managed dan Optimized. Perbaikan dilakukan secara bertahap berdasarkan tingkat risiko dan dievaluasi secara berkala untuk mendukung peningkatan keamanan, kerahasiaan, integritas, dan ketersediaan informasi RME.

REFERENSI

Ardianto, E. T., Sabran, S., & Nurjanah, L. (2024). Analisis aspek keamanan data pasien dalam implementasi rekam medis elektronik di Rumah Sakit X. Jurnal Rekam Medik & Manajemen Informasi Kesehatan, 3(2), 18–30. https://doi.org/10.47134/rmik.v3i2.54

Arif, A., Linawati, L., & Noak, P. A. (2026). Implementasi SNI ISO/IEC 27001:2022 terhadap perlindungan data rekam medis elektronik (RME) pada fasilitas pelayanan kesehatan di Indonesia. MAINTEKKES: The Journal of Management Information and Health Technology, 4(1), 1–8. https://doi.org/10.36049/qgkk3906

Asih, H. A., Indrayadi, I., Soraya, S., & Khairunnisa, K. (2024). Evaluasi keamanan data pasien pada rekam medis elektronik dengan systematic literature review. Jurnal Ilmiah FIFO, 16(2). https://doi.org/10.22441/fifo.2024.v16i2.001

Bahaudin, M. H., & Rizqi, A. W. (2024). Evaluasi Kesesuaian Penerapan Sistem Manajemen Keselamatan dan Kesehatan Kerja (SMK3) Berdasarkan ISO 45001: 2018 Menggunakan Metode Gap Analysis dan PDCA:(Studi kasus: PT Swabina Gatra). *Jurnal Teknologi dan Manajemen Industri Terapan*, *3*(I), 766-773. https://doi.org/10.55826/jtmit.v5i2.1716

Fathurohman, A., & Witjaksono, R. W. (2020). Analysis and design of information security management system based on ISO 27001: 2013 using Annex Control (Case Study: District of Government of Bandung City). *Bulletin of Computer Science and Electrical Engineering*, *1*(1), 1-11. https://doi.org/10.25008/bcsee.v1i1.2

Igayanti, I. B., Deviga, L., Mathar, I., & Ramadanintyas, K. N. (2026). TINJAUAN PENERAPAN REKAM MEDIS ELEKTRONIK BERBASIS E-LINK DI UPT PUSKESMAS MOJOPURNO. *Enfermeria Ciencia*, *4*(2), 148-169. https://doi.org/10.56586/ec.v4i2.113

Ikawati, F. R., & Ansyori, A. (2025). Literature Review: Analisis Keamanan Data Rekam Medis Elektronik di Fasilitas Kesehatan. *Jurnal Manajemen Informasi Kesehatan*

(Health Information Management), *10*(2), 230-237. https://doi.org/10.51851/jmis.v10i2.673

Ikawati, F. R., Ansyori, A., & Permatasari, D. A. S. (2025). Literature review: Analisis keamanan data rekam medis elektronik di fasilitas kesehatan. Jurnal Manajemen Informasi Kesehatan (Health Information Management), 10(2), 230–237. https://doi.org/10.51851/jmis.v10i2.673

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

International Organization for Standardization. (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.

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

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), 79–91. https://doi.org/10.36049/maintekkes.v3i2.420

Pramesti, D. P. A., Ayuningtyas, D., & Verdi, R. (2024). Keamanan dan kerahasiaan data medis pasien dalam implementasi rekam medis elektronik: Tinjauan sistematis. PREPOTIF: Jurnal Kesehatan Masyarakat, 8(3). https://doi.org/10.31004/prepotif.v8i3.38445

Rani, D. M., & Widyaningrum, B. N. (2025). Information security evaluation of the electronic medical records system at Sultan Agung Islamic Hospital. Jurnal Manajemen Informasi Kesehatan (Health Information Management), 10(1), 52–62. https://doi.org/10.51851/jmis.v10i1.636

Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Rumetna, M. S., Lina, T. N., Santoso, A. B., Karay, J., Komansilan, R., & Kaitelapatay, B. G. (2022). Pengetahuan serta peran auditor secara komprehensif dalam menghadapi dampak perkembangan teknologi informasi. *Jurnal Komtika (Komputasi dan Informatika)*, *6*(1), 26-38. https://doi.org/10.31603/komtika.v6i1.6776

Setyaningrum, E., & Ricky, A. V. (2025). Analisis keamanan data pasien dalam rekam medis elektronik berdasarkan CIA Triad di RSUD X Jawa Tengah. Jurnal Ners, 9(3), 4216–4221. https://doi.org/10.31004/jn.v9i3.46352

Simanullang, M. J., Aritonang, M. A. S., & Sinaga, F. M. (2026). Analisis Keamanan Data Pasien pada Sistem Informasi Manajemen Rumah Sakit (SIMRS). *Jurnal Desain Dan Analisis Teknologi*, *5*(1), 44-50. https://doi.org/10.58520/jddat.v5i1.98

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 (Jurnal Rekam Medis dan Informasi Kesehatan), 6(1). https://doi.org/10.58535/jrmik.v6i1.78

We'e, A., Nugroho, H., & Siswatibudi, H. (2023). Evaluasi aspek keamanan dan kerahasiaan rekam medis elektronik di Rumah Sakit Panti Nugroho. Jurnal Permata Indonesia, 14(2), 72–81. https://doi.org/10.59737/jpi.v14i2.265