ANALISIS KEPATUHAN SISTEM REKAM MEDIS ELEKTRONIK TERHADAP UNDANG UNDANG PERLINDUNGAN DATA PRIBADI DAN ISO 27000

ELECTRONIC MEDICAL RECORD SYSTEM COMPLIANCE WITH PERSONAL DATA PROTECTION LAW AND ISO 27000

Intan Dzikria[1], Rania Akila Nawa Dillah[2]
E-mail:[1)] intandzikria@untag-sby.ac.id, [2)] raniadillah21@gmail.com

[1]Sistem dan Teknologi Informasi, Fakultas Teknologi Elektro dan Informatika Cerdas, Universitas 17 Agustus 1945 Surabaya
[2]Teknik Informatika, Fakultas Teknologi Elektro dan Informatika Cerdas, Universitas 17 Agustus 1945 Surabaya

Abstrak

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan regulasi yang mengatur pengelolaan dan perlindungan data pribadi, termasuk data kesehatan yang bersifat sensitif. Dalam sektor kesehatan, penerapan Rekam Medis Elektronik (RME) menjadi salah satu upaya untuk meningkatkan efisiensi dan kualitas layanan kesehatan. Pengelolaan data pasien dalam sistem elektronik dapat menimbulkan tantangan terkait keamanan dan privasi data yang bersifat sensitif. Sehingga diperlukan evaluasi terhadap tingkat kepatuhan sistem terhadap ketentuan perlindungan data pribadi. Penelitian ini bertujuan untuk menganalisis tingkat kepatuhan salah satu sistem Rekam Medis Elektronik yang diterapkan di mengevaluasi pelayanan kesehatan, terhadap regulasi UU PDP dan ISO/IEC 27001 menggunakan pendekatan CIA Triad (*confiedientiality*, *integrity*, dan *availability*). Penelitian ini menggunakan teknik gap analysis untuk melakukan pemetaan UU PDP ke dalam tiga aspek CIA Triad. Proses evaluasi menggunakan standar keamanan informasi ISO/IEC 27001:2022, ISO/IEC 27002:2022, dan ISO/IEC 27701:2019 sebagai kerangka acuan dalam mendukung pemenuhan kepatuhan sistem terhadap UU PDP. Hasil penelitian memberikan gambaran mengenai tingkat kesesuaian sistem, sekaligus mengidentifikasi area pengelolaan keamanan dan privasi data kesehatan yang masih memerlukan perbaikan. Penelitian ini berkontribusi dengan menyediakan model evaluasi kepatuhan sistem RME terhadap UU PDP dan ISO 27000 yang terstruktur melalui integrasi pendekatan CIA Triad.

Kata kunci**:** *rekam medis elektronik, perlindungan data pribadi, cia triad, gap analysis*

Abstract

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is a regulation governing the management and protection of personal data, including sensitive health data. In the healthcare sector, the implementation of Electronic Medical Records (EMR) is one effort to improve the efficiency and quality of healthcare services. Managing patient data in electronic systems can pose challenges related to the security and privacy of sensitive data. Therefore, an evaluation of the system's compliance with personal data protection provisions is necessary. This study aims to analyze the compliance level of one of the Electronic Medical Records systems implemented in evaluating healthcare services, with the PDP Law and ISO/IEC 27001 regulations using the CIA Triad approach (confidentiality, integrity, and availability). This study uses a gap analysis technique to map the PDP Law into three aspects of the CIA Triad. The

evaluation process uses the information security standards ISO/IEC 27001:2022, ISO/IEC 27002:2022, and ISO/IEC 27701:2019 as a reference framework to support the system's compliance with the PDP Law. The research results provide an overview of the system's level of compliance and identify areas requiring improvement in health data security and privacy management. This research contributes by providing a structured model for evaluating the compliance of RME systems with the PDP Law and ISO 27000 through the integration of the CIA Triad approach

***Keywords**: electronic medical records, personal data protection, cia triad, gap analysis*

1. PENDAHULUAN

Perkembangan teknologi informasi mendorong meningkatnya penggunaan sistem elektronik dalam pengelolaan data, termasuk data pribadi yang bersifat sensitif. Dalam konteks ini, keamanan dan privasi data menjadi aspek krusial karena kebocoran data pribadi dapat menimbulkan risiko penyalahgunaan oleh pihak yang tidak bertanggung jawab [1]. Di sektor kesehatan, transformasi digital diwujudkan melalui penerapan Rekam Medis Elektronik (RME) yang memungkinkan pengelolaan data pasien secara lebih efisien dan terintegrasi. Namun, sistem ini juga menyimpan risiko tinggi terhadap pelanggaran keamanan informasi karena data medis bersifat rahasia.

Beberapa kasus kebocoran data di Indonesia, seperti insiden pada BPJS Kesehatan dan aplikasi e-HAC pada tahun 2021, menunjukkan adanya kerentanan dalam perlindungan data pribadi [1], [2]. Hal ini menegaskan pentingnya penerapan regulasi yang kuat dalam menjaga keamanan data. Pemerintah Indonesia telah menetapkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang mengatur kewajiban perlindungan data serta memastikan sistem elektronik beroperasi secara aman, andal, dan bertanggung jawab [3]. Selain itu, implementasi RME juga diatur dalam Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 sebagai bagian dari sistem informasi pelayanan kesehatan [4].

ISO/IEC 27001:2022, ISO/IEC 27002:2022, dan ISO/IEC 27701:2019 merupakan standar internasional yang digunakan dalam pengelolaan keamanan dan privasi informasi. Standar tersebut tidak hanya menyediakan kerangka kerja dalam penerapan sistem manajemen keamanan informasi, tetapi juga dapat membantu organisasi dalam memfasilitasi kepatuhan terhadap regulasi perlindungan data pribadi, termasuk Undang-Undang Pelindungan Data Pribadi (UU PDP) di Indonesia [5]. ISO/IEC 27001 berfokus pada sistem manajemen keamanan informasi [6], ISO/IEC 27002 memberikan panduan kontrol keamanan [7], sedangkan ISO/IEC 27701 memperluas cakupan ke manajemen informasi privasi.

Dalam penelitian ini, ketiga standar tersebut digunakan sebagai acuan pendukung dalam melakukan evaluasi pemenuhan sistem Rekam Medis Elektronik terhadap ketentuan dalam UU PDP. Penerapan standar ISO dilakukan melalui pemetaan pasal-pasal UU PDP ke dalam klausul ISO yang relevan, kemudian dianalisis lebih lanjut ke dalam aspek *Confidentiality, Integrity,* dan *Availability* (CIA). Dengan demikian, proses evaluasi tidak hanya mengacu pada regulasi nasional, tetapi juga selaras dengan standar internasional dalam keamanan dan privasi informasi.

Kemudian analisis keamanan informasi dapat dilakukan dengan pendekatan CIA Triad yang mencakup *confidentiality, integrity,* dan *availability* sebagai tiga prinsip utama dalam melindungi data [8]. Beberapa penelitian sebelumnya telah mengkaji keamanan RME menggunakan pendekatan CIA Triad dan mengacu pada regulasi yang berlaku [9]. Namun, penelitian yang secara khusus mengevaluasi kepatuhan sistem RME terhadap UU PDP masih

terbatas, sehingga diperlukan kajian lebih lanjut untuk menilai kesesuaian sistem dengan regulasi perlindungan data pribadi.

Penelitian ini bertujuan untuk menilai tingkat kepatuhan sistem Rekam Medis Elektronik terhadap ketentuan dalam UU PDP dan ISO 27000 serta memberikan rekomendasi perbaikan untuk meningkatkan keamanan dan perlindungan data pribadi. Evaluasi dilakukan dengan membandingkan kondisi aktual sistem dengan ketentuan dalam UU PDP dan ISO 27000 yang dipetakan berdasarkan konsep CIA Triad, sehingga diharapkan sistem RME tidak hanya mendukung efektivitas layanan kesehatan, tetapi juga memenuhi aspek keamanan informasi sesuai regulasi yang berlaku.

2. KAJIAN PUSTAKA

2.1 Rekam Medis Elektronik

Rekam Medis Elektronik (RME) merupakan sistem informasi yang digunakan untuk mengelola data pasien secara digital dalam fasilitas pelayanan kesehatan [4]. Penerapan RME dapat membantu dalam pengelolaan data yang lebih efisien, terintegrasi, serta mendukung ketepatan informasi medis dalam pengambilan keputusan. Namun, karena data yang dikelola bersifat sensitif, sistem ini memiliki risiko tinggi terhadap pelanggaran keamanan dan privasi data pasien sehingga memerlukan pengamanan yang memadai. Hal ini sejalan dengan penelitian yang dilakukan ole [9] yang menyatakan bahwa penerapan RME dapat meningkatkan efisiensi layanan kesehatan, namun tetap memerlukan pengamanan data yang memadai untuk melindungi informasi pasien.

2.2 Perlindungan Data Pribadi (UU PDP)

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) merupakan regulasi yang mengatur pengelolaan data pribadi di Indonesia [3]. UU PDP menetapkan kewajiban bagi pengendali data untuk memastikan keamanan data pribadi, mencegah akses tidak sah, serta menjamin bahwa pemrosesan data dilakukan secara bertanggung jawab. Dalam konteks layanan kesehatan, regulasi ini menjadi sangat penting karena data medis termasuk dalam kategori data pribadi yang bersifat sensitif. Pentingnya regulasi ini diperkuat oleh berbagai kasus kebocoran data di Indonesia, seperti insiden pada BPJS Kesehatan dan aplikasi e-HAC pada tahun 2021 yang menunjukkan adanya kerentanan dalam perlindungan data pribadi [1], [2].

2.3 Keamanan Informasi (CIA Triad)

Konsep *Confidentiality, Integrity,* dan *Availability* (CIA Triad) merupakan dasar dalam keamanan informasi yang digunakan untuk memastikan perlindungan data [10]. *Confidentiality* menekankan bahwa data hanya dapat diakses oleh pihak yang berwenang, *Integrity* memastikan data tetap akurat dan tidak berubah tanpa izin, sedangkan *Availability* menjamin bahwa data dapat diakses ketika dibutuhkan[11]. Konsep CIA ini juga digunakan dalam analisis keamanan sistem informasi, termasuk pada salah satu sistem Rekam Medis Elektronik di RSUD X Jawa Tengah untuk analisis keamanan data pasien [8]. Penelitian oleh [12] juga menggunakan pendekatan CIA Triad untuk mengevaluasi keamanan sistem RME, khususnya dalam menjaga kerahasiaan dan keutuhan data pasien.

2.4 Sandar Keamanan dan Privasi Informasi (ISO/IEC 27001, 27002, 27701)

ISO/IEC 27001:2022, ISO/IEC 27002:2022, dan ISO/IEC 27701:2019 merupakan standar internasional yang digunakan dalam pengelolaan keamanan dan privasi informasi. ISO/IEC 27001 berfokus pada sistem manajemen keamanan informasi [6], ISO/IEC 27002 memberikan panduan kontrol keamanan informasi [7], sedangkan ISO/IEC 27701 berfokus pada manajemen informasi privasi [13].

Standar tersebut dapat membantu organisasi dalam memfasilitasi kepatuhan terhadap regulasi perlindungan data pribadi, termasuk UU PDP di Indonesia [5]. Selain itu, standar ini memberikan panduan dalam menetapkan kebijakan, prosedur, serta pengendalian keamanan informasi untuk melindungi data pribadi.

Dalam konteks penelitian ini, standar ISO digunakan sebagai acuan pendukung untuk mengevaluasi pemenuhan sistem Rekam Medis Elektronik terhadap ketentuan UU PDP. Hal ini juga didukung oleh penelitian [5] yang menunjukkan bahwa terdapat keterkaitan antara ketentuan dalam UU PDP dengan standar ISO/IEC 27001:2022, ISO/IEC 27002:2022 dan ISO/IEC 27701:2019 dalam mendukung perlindungan data pribadi. Dengan demikian, penggunaan standar ISO dalam penelitian ini bertujuan untuk membantu pemenuhan kepatuhan sistem terhadap UU PDP serta dapat memastikan bahwa evaluasi kepatuhan sistem tidak hanya mengacu pada regulasi nasional, tetapi juga selaras dengan standar internasional dalam keamanan dan privasi informasi.

3. METODOLOGI

Penelitian ini menggunakan pendekatan kualitatif dengan metode *gap analysis* untuk menilai tingkat kepatuhan sistem Rekam Medis Elektronik (RME) terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP). Tahapan penelitian diawali dengan studi literatur untuk memperoleh landasan teori terkait UU PDP, konsep keamanan informasi *Confidentiality, Integrity, Availability* (CIA Triad), serta standar pendukung seperti ISO/IEC 27001, ISO/IEC 27002 dan ISO/IEC 27701. Penelitian ini menggunakan sebuah rekam medis elektronik (RME) XYZ untuk digunakan sebagai objek penelitian. Observasi dilakukan pada sistem RME XYZ untuk mengidentifikasi kondisi aktual pengelolaan dan keamanan data pada sistem.

Tahap berikutnya adalah pemetaan pasal-pasal dalam UU PDP dan ISO 27000 ke dalam aspek CIA Triad sebagai dasar penyusunan kriteria penilaian. Pemilihan pasal UU PDP mengacu pada [5] serta relevansi dengan standar keamanan informasi untuk memastikan kesesuaian antara regulasi dan praktik implementasi untuk membantu memenuhi kepatuhan sistem tehadap UU PDP [5]. Hasil pemetaan kemudian digunakan untuk menyusun skenario pengujian dalam bentuk kategori terpenuhi dan tidak terpenuhi yang berfungsi sebagai instrumen evaluasi terhadap sistem.

Pengumpulan data dilakukan melalui tiga teknik utama, yaitu observasi, studi literatur, dan wawancara. Observasi digunakan untuk mengamati secara langsung fitur dan mekanisme keamanan pada sistem RME XYZ, sedangkan studi literatur digunakan untuk memperkuat landasan teori dan standar yang digunakan dalam penelitian. Wawancara dilakukan kepada pihak yang terlibat dalam pengelolaan sistem untuk memperoleh informasi terkait kebijakan, prosedur, dan dokumentasi yang tidak dapat diamati secara langsung. Hasil wawancara digunakan sebagai pelengkap dalam proses pengujian agar data yang diperoleh lebih valid.

Analisis data dilakukan menggunakan metode *gap analysis* dengan membandingkan kondisi aktual sistem dengan kondisi ideal berdasarkan UU PDP dan ISO 27000 yang telah dipetakan ke dalam CIA Triad. Hasil analisis berupa identifikasi kesenjangan (gap) yang menunjukkan tingkat kesesuaian sistem terhadap regulasi, serta aspek-aspek yang masih

memerlukan perbaikan. Berdasarkan temuan tersebut, disusun rekomendasi untuk meningkatkan keamanan dan kepatuhan sistem RME terhadap perlindungan data pribadi.

4. HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk menilai tingkat kepatuhan sistem Rekam Medis Elektronik terhadap ketentuan dalam Undang-Undang Pelindungan Data Pribadi (UU PDP) serta memberikan rekomendasi perbaikan untuk meningkatkan keamanan dan perlindungan data pribadi pada sistem.

Pemetaan pasal-pasal dalam UU PDP ke dalam standar ISO beserta klausulnya dilakukan dengan mengacu pada penelitian [5] yang mengkaji keterkaitan antara regulasi perlindungan data pribadi dengan standar ISO/IEC 27001:2022, ISO/IEC 27002:2022 dan ISO/IEC 27701:2019. Selanjutnya, pemetaan dari klausul ISO ke dalam aspek *Confidentiality, Integrity,* dan *Availability* (CIA Triad) dilakukan melalui studi literatur terhadap dokumen standar ISO/IEC 27001:2022, ISO/IEC 27002:2022, dan jurnal terkait ISO/IEC 27701:2019. Pemetaan tersebut digunakan sebagai dasar dalam penyusunan instrumen evaluasi yang ditunjukkan pada Tabel 1.

Tabel 1. Pemetaan UU PDP berdasarkan CIA

Pasal UU PDP	ISO/Klausul	CIA
40-45	27002:2022 / 8.10	C
46-47	27002:2022 / 5.24, 5.25, 5.26	CIA
49	27002:2022 / 5.31	CIA
50	27002:2022 / 5.31	CIA
53-54	27002:2022 / 5.34	CIA
55-56	27002:2022 / 5.14	CIA
65-66	27002:2022 / 5.33, 5.34, 8.12	CIA
35-39	27001:2022 /4–9	CIA
19-24	27701:2019 / 7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.3.2, 7.3.3	C
25-26	27701:2019 / 7.2.2, 7.2.3, 7.3.3	C
27-33	27701:2019 / 7.2.1, 7.2.2, 7.2.8, 7.3.2, 7.3.3, 7.3.6, 7.3.8, 7.4.2	CIA
34	27701:2019 / 7.2.5	C
48	27701:2019 / 8.4.2 dan 8.5	CIA
51-52	27701:2019 / 7.2.6 dan 8	CI

Hasil penelitian ini diperoleh melalui proses pengujian kepatuhan sistem Rekam Medis Elektronik (RME) XYZ terhadap ketentuan Undang-Undang Perlindungan Data Pribadi (UU PDP) yang telah dipetakan berdasarkan aspek *Confidentiality, Integrity,* dan *Availability* (CIA). Pengujian tersebut didukung dengan pembuatan 137 Skenario pengujian, dengan sample skenario seperti yang ditunjukkan pada Tabel 2.

Tabel 2. Skenario Pengujian Kepatuhan RME terhadap UU PDP

Pasal UU PDP	**27-33**
ISO/Klausul	27701:2019 / 7.2.1, 7.2.2,7.2.8, 7.3.2, 7.3.3, 7.3.6, 7.3.8, 7.4.2
Tujuan	Memastikan pemrosesan data pribadi dilakukan secara sah, transparan, terbatas, serta mendukung hak akses dan perbaikan data oleh subjek data.

Prosedur Pengujian	Melakukan pemeriksaaan dokumen kebijakan pemrosesan data, pengujian input dan pembaruan data pasien pada sistem, serta verifikasi ketersediaan informasi hak subjek data dan pencatatan aktivitas.
Hasil yang Diharapkan	Sistem mampu memproses data sesuai tujuan, menyediakan transparansi informasi, menjaga keakuratan data, serta mencatat seluruh aktivitas pemrosesan data.
CIA	CIA (*Confidentiality*, *Integrity*, dan *Availability*)
Pasal UU PDP	**40-45**
ISO/Klausul	27002:2022 / 8.10
Tujuan	Memastikan data pribadi pada sistem rekam medis elektronik dapat dihapus secara aman ketika data tersebut tidak lagi diperlukan.
Prosedur Pengujian	Melakukan pemeriksaan dokumen kebijakan retensi dan penghapusan data pribadi, melakukan simulasi penghapusan data pasien pada sistem oleh pengguna yang berwenang, serta memverifikasi bahwa data yang telah dihapus tidak lagi dapat diakses dan aktivitas penghapusan tercatat pada log sistem.
Hasil yang Diharapkan	Sistem mampu menghapus data pribadi secara aman sesuai kebijakan yang berlaku, data yang telah dihapus tidak dapat diakses kembali, serta proses penghapusan tercatat sebagai bukti pelaksanaan penghapusan data.
CIA	C (*Confidentiality*)
Pasal UU PDP	**51-52**
ISO/Klausul	27701:2019 / 7.2.6 dan 8
Tujuan	Memastikan pemrosesan data pribadi oleh prosesor dilakukan sesuai instruksi pengendali data, menjaga keamanan dan kerahasiaan data, serta mencatat aktivitas pemrosesan data.
Prosedur Pengujian	Melakukan pemeriksaan dokumen kebijakan atau perjanjian antara pengendali dan prosesor data, melakukan pengujian akses dan aktivitas pemrosesan data pasien oleh pengguna pada sistem, serta memverifikasi pembatasan akses sesuai peran, pencatatan aktivitas pada log sistem, dan penerapan mekanisme keamanan dalam pemrosesan data.
Hasil yang Diharapkan	Sistem memastikan pemrosesan data pribadi hanya dilakukan sesuai instruksi pengendali, aktivitas pemrosesan tercatat dengan baik, serta data dilindungi melalui mekanisme keamanan dan pembatasan akses.
CIA	CI (*Confidentiality* dan *Integrity*)
Pasal UU PDP	**46-47**
ISO/Klausul	27002:2022 / 5.24, 5.25, 5.26
Tujuan	Memastikan sistem rekam medis elektronik memiliki mekanisme pencatatan, penanganan, dan pelaporan insiden keamanan informasi yang berkaitan dengan kegagalan perlindungan data pribadi.
Prosedur Pengujian	Melakukan pengujian akses pada sistem rekam medis elektronik untuk memverifikasi ketersediaan fitur pencatatan insiden keamanan informasi, mensimulasikan percobaan akses tidak sah terhadap data pasien, serta memeriksa pencatatan kejadian pada log sistem dan mekanisme penanganan serta pelaporan insiden.

Hasil yang Diharapkan	Sistem mampu mencatat, mengklasifikasi, dan menangani insiden keamanan informasi serta menyediakan mekanisme pelaporan insiden sesuai dengan prosedur yang berlaku.
CIA	CIA (*Confidentiality*, *Integrity*, dan *Availability*)

Tabel 2 menunjukkan sample skenario pengujian pada beberapa pasal UU PDP yang mencakup aspek confidentiality, integrity, dan availability (CIA). Skenario pengujian ini digunakan untuk mengevaluasi kesesuaian antara kondisi aktual sistem dengan ketentuan yang berlaku dalam UU PDP dengan menggunakan standar keamanan informasi sebagai acuan pendukung, yaitu ISO/IEC 27001:2022, ISO/IEC 27002:2022, dan ISO/IEC 27701:2019. Tabel tersebut hanya menampilkan sebagian sample skenario pengujian, sedangkan pengujian dilakukan pada seluruh pasal yang dipetakan. Hasil pengujian kemudian diklasifikasikan ke dalam kategori terpenuhi dan tidak terpenuhi. Ringkasan hasil pengujian kepatuhan sistem berdasarkan kelompok pasal disajikan pada Tabel 3.

Tabel 3. Ringkasan Hasil Pengujian

Pasal	ISO/IEC	Aspek	Total Prosedur	Terpenuhi	Tidak Terpenuhi	Tingkat Kepatuhan
40-45	27002:2022	C	6	4	2	66,7%
46-47	27002:2022	CIA	6	2	4	33,3%
49	27002:2022	CIA	6	5	1	83,3%
50	27002:2022	CIA	5	1	4	20%
53-54	27002:2022	CIA	6	4	2	66,7%
55-56	27002:2022	CIA	6	3	3	50%
65-66	27002:2022	CIA	6	3	3	50%
35-39	27001:2022	CIA	25	6	19	24%
19-24	27701:2019	C	13	11	2	84,6%
25-26	27701:2019	C	13	9	4	69,2%
27-33	27701:2019	CIA	18	12	6	66,7%
34	27701:2019	C	8	3	5	37,5%
48	27701:2019	CIA	8	4	4	50%
51-52	27701:2019	CI	11	6	5	54,5%

Berdasarkan hasil pengujian kepatuhan sistem RME XYZ terhadap UU PDP yang telah dipetakan ke dalam aspek *Confidentiality, Integrity, Availability* (CIA), diperoleh tingkat kepatuhan yang bervariasi pada setiap kelompok pasal. Secara umum, sistem menunjukkan tingkat kepatuhan yang cukup baik pada beberapa pasal seperti Pasal 19–24 (84,6%) dan Pasal 49 (83,3%), yang menunjukkan mekanisme operasional seperti persetujuan, pembatasan akses, serta kepatuhan terhadap regulasi dasar telah diterapkan dengan cukup baik. Namun, masih terdapat beberapa pasal dengan tingkat kepatuhan rendah, seperti Pasal 50 (20%) dan Pasal 35–39 (24%), yang menunjukkan bahwa aspek kebijakan, dokumentasi, serta manajemen keamanan informasi belum diterapkan secara optimal.

Hasil penelitian ini menunjukkan bahwa sebagian besar kekuatan sistem terletak pada implementasi teknis, seperti autentikasi login, pembatasan akses berdasarkan peran, serta pengelolaan data pada tingkat operasional. Hal ini dapat dilihat dari beberapa pasal dengan nilai menengah hingga tinggi, seperti Pasal 27–33 (66,7%), Pasal 40–45 (66,7%), dan Pasal 53–54 (66,7%). Namun, kelemahan utama sistem terletak pada kurangnya dukungan kebijakan resmi, prosedur tertulis, serta pencatatan aktivitas. Pada pasal yang memiliki nilai rendah hingga sedang ditemukan bahwa sistem belum memiliki dokumentasi resmi terkait perlindungan data pribadi, belum tersedia mekanisme pencatatan aktivitas pengguna, serta belum terdapat prosedur penanganan insiden keamanan informasi. Kondisi ini berpotensi menghambat proses pemantauan, audit, serta penelusuran aktivitas dalam sistem.

Selain itu, aspek manajemen keamanan informasi secara menyeluruh juga masih belum terpenuhi, terutama pada Pasal 35–39 yang berkaitan dengan penerapan sistem manajemen keamanan informasi. Meskipun beberapa kontrol teknis telah diterapkan, seperti pembatasan akses dan pengendalian perubahan data, namun belum terdapat kebijakan resmi, manajemen risiko dan audit internal. Ditemukan juga pada pengelolaan transfer data di mana implementasi teknis sudah tersedia tetapi belum didukung oleh kebijakan dan prosedur yang terdokumentasi dengan baik.

Secara keseluruhan, dari total prosedur pengujian 137 yang dilakukan diperoleh 73 prosedur pengujian terpenuhi dan 64 prosedur pengujian tidak terpenuhi. Berdasarkan hasil tersebut, tingkat kepatuhan sistem terhadap ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi adalah sebesar 53,3%.

Berdasarkan hasil penelitian, dapat disimpulkan bahwa sistem RME XYZ telah memenuhi sebagian aspek kepatuhan terhadap UU PDP, khususnya pada implementasi teknis dan operasional. Namun, untuk mencapai kepatuhan yang lebih optimal, diperlukan penguatan pada aspek tata kelola keamanan informasi, terutama dalam penyusunan kebijakan resmi, dokumentasi prosedur, pencatatan aktivitas sistem, serta penerapan manajemen keamanan informasi secara menyeluruh. Peningkatan pada aspek-aspek tersebut diharapkan dapat mendukung kepatuhan sistem terhadap UU PDP serta pemenuhan prinsip *confidentiality, integrity,* dan *availability* secara lebih menyeluruh serta meningkatkan perlindungan data pribadi dalam sistem RME.

5. KESIMPULAN DAN SARAN

Penelitian ini bertujuan untuk menilai tingkat kepatuhan sistem Rekam Medis Elektronik terhadap ketentuan dalam Undang-Undang Pelindungan Data Pribadi (UU PDP) dengan menggunakan pendekatan *gap analysis* berbasis aspek *Confidentiality, Integrity,* dan *Availability* (CIA), serta mengacu pada standar ISO/IEC 27001:2022, ISO/IEC 27002:2022, dan ISO/IEC 27701:2019 sebagai acuan dalam pengelolaan keamanan dan privasi informasi. Hasil penelitian menunjukkan bahwa tingkat kepatuhan sistem mencapai 53,3%, yang menyatakan bahwa sistem baru memenuhi sebagian ketentuan perlindungan data pribadi.

Tingkat kepatuhan yang relatif tinggi ditemukan pada aspek teknis, seperti mekanisme persetujuan dan pemrosesan data, yang menunjukkan bahwa sebagian kontrol operasional telah diterapkan dan sejalan dengan praktik pengendalian dalam standar ISO. Namun demikian, tingkat kepatuhan yang rendah masih terdapat pada aspek kebijakan, dokumentasi, dan manajemen keamanan informasi. Hal ini menunjukkan bahwa penerapan kontrol berbasis ISO, khususnya yang berkaitan dengan sistem manajemen keamanan informasi dan pengelolaan risiko, belum diimplementasikan secara optimal.

Oleh karena itu, diperlukan upaya peningkatan melalui penyusunan kebijakan keamanan informasi secara terdokumentasi, penerapan mekanisme pencatatan aktivitas (*audit log*), serta pengelolaan risiko keamanan informasi yang mengacu pada standar ISO. Dengan demikian, penerapan standar ISO tidak hanya berfungsi sebagai acuan, tetapi juga sebagai langkah strategis dalam meningkatkan kepatuhan terhadap UU PDP.

Penelitian ini berkontribusi secara akademis pada pengembangan kajian evaluasi kepatuhan sistem Rekam Medis Elektronik dengan mengintegrasikan regulasi perlindungan data pribadi dan standar keamanan informasi ISO ke dalam kerangka analisis berbasis *Confidentiality, Integrity,* dan *Availability* (CIA). Sedangkan kontribusi penelitian ini secara praktis adalah sebagai bahan evaluasi bagi pengelola sistem dalam mengidentifikasi kelemahan serta meningkatkan penerapan keamanan informasi dan perlindungan data pribadi agar lebih sesuai dengan regulasi dan standar yang berlaku.

6. DAFTAR RUJUKAN

[1] C. Sorisa *et al.*, “Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia,” *J. Sains Student Res.*, vol. 2, no. 6, pp. 586–593, 2024, Accessed: May 04, 2026. [Online]. Available: https://doi.org/10.61722/jssr.v2i6.2996

[2] A. Nadiroh and S. A. Wiraguna, “Analisis Yuridis Kebocoran Data di Layanan Kesehatan Digital: Studi Kasus Aplikasi Telemedicine di Indonesia,” *Media Huk. Indones.*, vol. 2, no. 6, pp. 313–320, 2025, Accessed: May 04, 2026. [Online]. Available: https://doi.org/10.5281/zenodo.15520536

[3] “Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.” Accessed: May 04, 2026. [Online]. Available: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

[4] Kementerian Kesehatan Republik Indonesia, “Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis.” Accessed: May 04, 2026. [Online]. Available: https://peraturan.go.id

[5] E. Aristianto, M. H. Hilman, and S. Yazid, “Evaluating ISO Standards for Indonesian PDP Law Compliance: A Regulatory Mapping and Literature Review,” *Sci. J. Informatics*, vol. 12, no. 1, pp. 145–158, 2025.

[6] ISO/IEC, “Information security, cybersecurity and privacy protection --- Information security management systems --- Requirements,” 2022, *Geneva, Switzerland*.

[7] ISO/IEC, “Information security, cybersecurity and privacy protection --- Information security controls,” 2022, *Geneva, Switzerland*.

[8] E. Setyaningrum and A. V. Ricky, “Analisis Keamanan Data Pasien dalam Rekam Medis Elektronik Berdasarkan Cia Triad di RSUD X Jawa Tengah,” *J. Ners*, vol. 9, no. 3, pp. 4216–4221, 2025, doi: 10.31004/jn.v9i3.46352.

[9] U. S. Suhariyono, F. Rusdian Ikawati, and N. Afifah, “Analisis Aspek Keamanan Informasi Data Pasien pada Rekam Medis Elektronik di UPT Puskesmas Karangploso,” *J. Manaj. Inf. Kesehat. Indones.*, vol. 13, no. 1, pp. 2337–585, 2025.

[10] O. Mitchell, C. Osazuwa, G. Cpss, and C. S. S. Fty, “Confidentiality, Integrity, and

Availability in Network Systems: A Review of Related Literature," *Int. J. Innov. Sci. Res. Technol.*, vol. 8, no. 12, 2023.

[11] ISO/IEC, "Information technology --- Security techniques --- Information security management systems --- Overview and vocabulary," 2018, *Geneva, Switzerland*.

[12] S. W. Widiyanti *et al.*, "Tinjauan Keamanan Data Rekam Medis Elektronik Pada Aplikasi Simpus Berdasarkan Aspek Confidentiality, Integrity, Dan Availability Di Puskesmas Tasikmadu Karanganyar," *Indones. J. Heal. Inf. Manag.*, vol. 4, no. 2, pp. 1–6, 2024, Accessed: May 04, 2026. [Online]. Available: https://ijhim.stikesmhk.ac.id/ojsdata/article/view/212/94

[13] I. O. for Standardization and I. E. Commission, "Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance," ISO/IEC 27701. Accessed: May 04, 2026. [Online]. Available: https://www.iso.org/standard/71670.html