Volume 4 Nomor 1 (2026) 1-8

The Journal of Management Information and Health Technology
e-ISSN: 3025 - 2962

Implementasi SNI ISO/IEC 27001:2022 Terhadap Perlindungan Data Rekam Medis Elektronik (RME) Pada Fasilitas Pelayanan Kesehatan Di Indonesia

Arif Susanto[1] ,Linawati[2], Piers Andreas Noak[3]

[1]*Magister Hukum Kesehatan, Pascasarjana, Universitas Udayana; Magister Kesehatan Masyarakat, Pascasarjana, Universitas Hang Tuah Pekanbaru; Magister Kesehatan Masyarakat, Fakultas Ilmu dan Teknologi Kesehatan, Universitas Jenderal Achmad Yani*,
[2]*Program Studi Teknik Elektro, Fakultas Teknik, Universitas Udayana,*
[3]*Magister Hukum Kesehatan, Pascasarjana, Universitas Udayana.*

Corresponding author: Arif Susanto
Email: arif@htp.ac.id

ABSTRAK

Penerapan Rekam Medis Elektronik (RME) pada fasilitas pelayanan kesehatan (fasyankes) di Indonesia dapat menjadi kerangka kewajiban normatif yang ditetapkan melalui regulasi sektor kesehatan, dan diperkuat oleh Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Data kesehatan dikategorikan sebagai data pribadi spesifik dengan tingkat perlindungan tinggi. SNI ISO/IEC 27001:2022 sebagai standar nasional keamanan informasi dipandang cukup relevan untuk mendukung perlindungan data RME melalui penerapan Sistem Manajemen Keamanan Informasi (SMKI) karena berbasis manajemen risiko. Penelitian ini bertujuan mengkaji secara kritis implementasi SNI ISO/IEC 27001:2022 terhadap perlindungan data RME pada fasyankes di Indonesia dari perspektif hukum normatif. Metode yang digunakan adalah *systematic literature review* berbasis protokol PRISMA dengan kerangka kerja (*framework*) *Theory-Context-Characteristics-Methodology* (TCCM). Hasil kajian menunjukkan bahwa mayoritas literatur masih memposisikan SNI ISO/IEC 27001:2022 sebagai instrumen teknis dan administratif, tanpa mengaitkannya secara eksplisit dengan pemenuhan kewajiban hukum berdasarkan UU PDP. Implementasi SMKI memiliki kecenderungan berorientasi pada kepatuhan prosedural dan sertifikasi, sementara perlindungan substantif terhadap hak privasi pasien belum menjadi fokus utama. Temuan ini menegaskan bahwa kepatuhan terhadap SNI ISO/IEC 27001:2022 belum memiliki sifat *legal safe harbour*, tetapi hanya dapat berfungsi sebagai bukti *due diligence* yang harus diintegrasikan dengan tata kelola kepatuhan hukum untuk menjamin perlindungan data RME secara komprehensif.

Kata Kunci: fasyankes, perlindungan data, rekam medis elektronik (RME), SNI ISO/IEC 27001:2022.

ABSTRACT

The implementation of Electronic Medical Records (EMR) in healthcare facilities in Indonesia can be understood as a normative obligation framework established through health sector regulations and reinforced by Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). Health data are classified as specific personal data requiring a high level of protection. SNI ISO/IEC 27001:2022, as a national information security standard, is considered sufficiently relevant to support the protection of EMR data through the implementation of an Information Security Management System (ISMS), as it is based on a risk management approach. This study aims to critically examine the implementation of SNI ISO/IEC 27001:2022 in protecting EMR data in Indonesian healthcare facilities from a normative legal perspective. The method employed is a systematic literature review based on the PRISMA protocol, utilizing the Theory–Context–Characteristics–Methodology (TCCM) framework.

The findings indicate that the majority of the literature still positions SNI ISO/IEC 27001:2022 as a technical and administrative instrument, without explicitly linking it to the fulfilment of legal obligations under the PDP Law. The implementation of ISMS tends to be oriented toward procedural compliance and certification, while substantive protection of patient privacy rights has not yet become the primary focus. These findings affirm that compliance with SNI ISO/IEC 27001:2022 does not constitute a legal safe harbour, but rather serves as evidence of due diligence, which must be integrated with legal compliance governance to ensure comprehensive protection of EMR data.
Keyword: *data protection, health service facilities, electronic medical record* (EMR), SNI ISO/IEC 27001:2022.

PENDAHULUAN

Transformasi digital pada sektor kesehatan di Indonesia telah memasuki fase normatif dengan adanya kewajiban penerapan Rekam Medis Elektronik (RME) pada seluruh fasilitas pelayanan kesehatan (fasyankes). Kewajiban tersebut ditetapkan melalui Peraturan Menteri Kesehatan (PMK) Nomor 24 Tahun 2022 (Kementerian Kesehatan RI, 2022), Surat Edaran (SE) Menteri Kesehatan Nomor HK.02.01/MENKES/1030/2023 (Kementerian Kesehatan RI, 2023), dan SE Direktur Jenderal Kesehatan Lanjutan Nomor RS.01.04/D/6199/2025 (Kementerian Kesehatan RI, 2025). Pada 11 Maret 2026, Direktorat Jenderal Kesehatan Lanjutan, Kementerian Kesehatan RI menerbitkan Surat edaran terbaru dengan Nomor YM.02.02/D/9/971/2026 tentang Pemberian Sanksi terhadap Penyelenggaraan RME di Rumah Sakit (Kementerian Kesehatan RI, 2026).

Regulasi tersebut menekankan bahwa pengelolaan data rekam medis (RM) harus dilakukan secara elektronik berupa RME, dalam rangka meningkatkan efisiensi pelayanan, kesinambungan perawatan, serta integrasi dengan sistem kesehatan nasional (SKN). Namun, digitalisasi layanan kesehatan secara simultan meningkatkan tingkat paparan risiko terhadap keamanan informasi, mengingat pengelolaan RME melibatkan volume besar data kesehatan yang bersifat sangat sensitif (Kementerian Kesehatan RI, 2022). Hal ini disebabkan karena data RME tentu mengandung informasi kesehatan individual, di mana oleh hukum Indonesia data tersebut dikategorikan sebagai data pribadi spesifik. Dengan demikian, maka diperlukan tingkat perlindungan yang lebih tinggi dibandingkan dengan data pribadi umum. Perihal inipun telah ditegaskan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

UU PDP menempatkan data kesehatan sebagai objek perlindungan khusus, dan menetapkan kewajiban hukum yang ketat bagi pengendali data. Dalam konteks tersebut, maka fasyankes diposisikan sebagai pengendali data pribadi yang bertanggung jawab secara hukum atas terjaminnya keamanan data pasien, termasuk apabila terjadi kegagalan perlindungan atau pelanggaran data (Republik Indonesia, 2022). Sejalan dengan rezim hukum tersebut, Indonesia telah menetapkan SNI ISO/IEC 27001:2022 sebagai Standar Nasional Indonesia (SNI) melalui Badan Standardisasi Nasional (BSN) dengan status adopsi identik (*identical adoption*) dari ISO/IEC 27001:2022 yang dikeluarkan oleh *International Organization for Standardization* (ISO). Standar ini berfungsi sebagai kerangka kerja nasional dalam pembangunan Sistem Manajemen Keamanan Informasi (SMKI) yang berbasis manajemen risiko, dan berorientasi pada perlindungan kerahasiaan, keutuhan, serta ketersediaan informasi (BSN, 2023).

SNI ISO/IEC 27001:2022 dengan statusnya sebagai SNI yang berlaku, maka standar ini tidak hanya bersifat teknis, tetapi juga memiliki legitimasi nasional sebagai standar acuan tata kelola maupun SMKI lintas sektor, termasuk terhadap sektor kesehatan. Dalam perspektif hukum, keberadaan SNI ISO/IEC 27001:2022 memiliki relevansi langsung terhadap pelaksanaan kewajiban dalam UU PDP. Meskipun UU PDP tidak mewajibkan penggunaan satu standar teknis tertentu, penerapan SNI ISO/IEC 27001:2022 dapat dipandang sebagai bentuk upaya kepatuhan dan kehati-hatian (*due diligence*) oleh fasyankes dalam memenuhi kewajiban hukum perlindungan data pribadi. Dengan demikian, SMKI berdasarkan SNI ISO/IEC 27001:2022 berpotensi menjadi instrumen pendukung pembuktian kepatuhan terhadap prinsip akuntabilitas dan pengamanan data sebagaimana diatur dalam UU PDP.

Namun, praktik implementasi SNI ISO/IEC 27001:2022 pada fasyankes berupa rumah sakit (RS) menunjukkan adanya kecenderungan reduksi makna standar, bahkan cenderung menjadi sekadar pemenuhan administratif dan sertifikasi formal. Banyak organisasi berfokus pada penyusunan dokumen, pengendalian teknis, dan kepatuhan audit. Sementara itu, integrasi standar dengan aspek manajemen risiko hukum, penguatan kesadaran sumber daya manusia kesehatan (SDMK), dan budaya keamanan organisasi masih belum optimal. Kondisi ini kemudian memiliki potensi menimbulkan kesenjangan antara kepatuhan (*compliance*) terhadap standar nasional dan perlindungan substantif terhadap hak privasi pasien yang dijamin oleh hukum (ISO/IEC, 2022). Ketidaksinkronan tersebut menunjukkan bahwa penerapan SNI ISO/IEC 27001:2022 tidak dapat dipahami sebagai jaminan absolut terhadap pemenuhan kewajiban hukum dalam UU PDP.

Sebaliknya, standar ini harus diposisikan sebagai bagian dari tata kelola *digital health* yang lebih luas, di mana keamanan informasi, kepatuhan hukum, dan faktor manusia saling terkait dan mempengaruhi. Tanpa adanya pendekatan integratif, fasyankes tetap menghadapi risiko kebocoran data dan tanggung jawab hukum, meskipun telah menerapkan atau disertifikasi berdasarkan SNI ISO/IEC 27001:2022 (WHO, 2021). Adanya kompleksitas hubungan antara kewajiban hukum perlindungan data pribadi yaitu UU PDP dan penerapan standar nasional keamanan informasi SNI ISO/IEC 27001:2022 menunjukkan bahwa perlindungan data RME tidak dapat dipahami secara parsial. Kajian terhadap isu ini melibatkan berbagai dimensi, mulai dari standar teknis keamanan informasi, tata kelola organisasi, faktor manusia, hingga implikasi yuridis terhadap tanggung jawab fasyankes.

Perkembangan penelitian terkait implementasi SNI ISO/IEC 27001:2022 dalam konteks RME di Indonesia masih terbatas serta menunjukkan keragaman fokus, pendekatan metodologis, dan kedalaman analisis, sehingga menyulitkan penarikan kesimpulan yang komprehensif dan terintegrasi. Dalam konteks tersebut, pendekatan kajian literatur sistematik (*systematic literature review*) menjadi relevan dan strategis yang memungkinkan peneliti mampu mengidentifikasi pola implementasi, kecenderungan metodologis, serta kesenjangan penelitian (*research gaps*) terkait penerapan SNI ISO/IEC 27001:2022 terhadap perlindungan data RME pada fasyankes di Indonesia. Melalui SLR ini, hubungan antara kepatuhan terhadap standar keamanan informasi dan pemenuhan kewajiban hukum berdasarkan UU PDP dapat dianalisis secara lebih objektif dan berbasis bukti ilmiah.

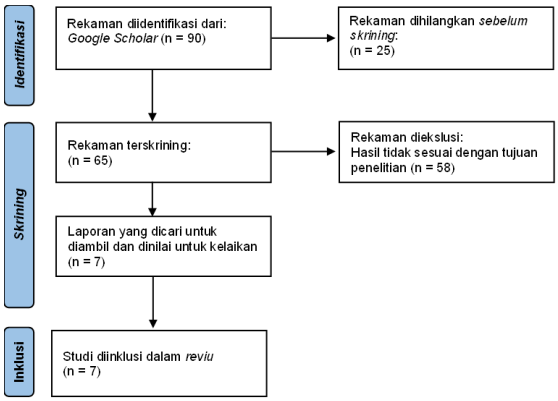
Berdasarkan uraian tersebut, penelitian ini dilakukan untuk mengkaji secara kritis implementasi SNI ISO/IEC 27001:2022 terhadap perlindungan data RME pada fasyankes di Indonesia, khususnya dalam kaitannya dengan pemenuhan kewajiban hukum berdasarkan UU PDP. Kajian ini diharapkan dapat memberikan pemahaman yang lebih komprehensif mengenai peran standar nasional keamanan informasi dalam mendukung perlindungan hak pasien, memperkuat tata kelola *digital health*, serta menjembatani pendekatan teknis dan yuridis dalam pengelolaan RME.

METODE PENELITIAN

Metode penelitian ini menggunakan *systematic literature review* (SLR) berbasis protokol *Preferred Reporting Items for Systematic Reviews and Meta-analyses* (PRISMA) untuk menelaah secara kritis literatur terkait implementasi SNI ISO/IEC 27001:2022 pada RME di Indonesia. Data yang diperoleh dan digunakan yaitu jurnal yang diakses melalui basis data elektronik yang tersedia di *Google Scholar (GS)* karena difokuskan terhadap implementasi SNI ISO/IEC 27001:2022 pada fasyankes. Pendekatan ini dipilih untuk menjawab keterbatasan penelitian sebelumnya yang cenderung menempatkan standar keamanan informasi dan kewajiban hukum secara terpisah. Selain itu, penelitian hanya dibatasi pada penelitian yang berada di wilayah Indonesia. Kriteria inklusi terdiri dari penggunaan ISO 27001:2022, sedangkan penggunaan ISO 27001 versi 2013 masuk ke dalam kriteria ekslusi.

Kriteria ekslusi lainnya terdiri atas: 1) bukan merupakan artikel ilmiah seperti laporan kerja praktik lapangan atau magang, 2) laporan tugas akhir berupa skripsi, dan 3) bentuk laporan lainnya, 4) judul dan abstrak yang tidak sesuai dengan tujuan penelitian. Penilaian kualitas artikel ilmiah dibantu dengan daftar periksa (*checklist*) sesuai dengan PRISMA 2020 yang terdiri atas 27 item pemeriksaan.

Pencarian data disesuaikan dengan *string* yang terdiri atas: "Implementasi" AND "ISO/IEC 27001" AND "perlindungan" AND "data pasien" OR "rekam medis elektronik" AND "fasilitas pelayanan kesehatan" OR "puskesmas" OR "rumah sakit" AND "INDONESIA". Selanjutnya artikel ilmiah yang diperoleh kemudian dilakukan penelaaahan pendahuluan terhadap abstrak dan keseluruhan naskah untuk menentukan apakah sesuai dengan tujuan penelitian.



Gambar 1. Hasil Skrining Literatur berdasarkan Diagram Alir PRISMA

Kerangka kerja (*framework*) *Theory - Context - Characteristics - Methodology* (TCCM) digunakan dalam SLR ini. Kerangka kerja ini dinilai memungkinkan dapat dilakukan pemetaan literatur secara sistematis berdasarkan landasan teoretis yang digunakan, konteks fasyankes, karakteristik implementasi SNI ISO/IEC 27001:2022, serta metode penelitian yang diterapkan. Gambar 1 menunjukkan hasil dari seluruh jurnal yang sesuai dengan *string* yang ditetapkan. Melalui tahap *skrining* awal, terdapat sebanyak 90 jurnal, kemudian sebanyak 25 jurnal dihilangkan karena tidak sesuai dengan tujuan penelitian, sehingga menyisakan 65 jurnal. Dari 65 jurnal yang tersisa tersebut, kemudian dilakukan *skrining* lanjutan yang mengeliminasi 58 artikel tambahan. Rincian hasil *skrining* tersebut dieliminasi karena sesuai dengan kriteria ekslusi, yaitu bukan merupakan artikel ilmiah dan memiliki judul dan abstrak yang tidak sesuai dengan tujuan penelitian. Selanjutnya, 7 artikel yang lolos dianalisis kelaikan *fulltext.* Akhirnya diperoleh 7 artikel yang terinklusi atau laik untuk digunakan dalam penelitian.

HASIL DAN PEMBAHASAN

Tabel 1 menujukkan hasil analisis menggunakan kerangka kerja TCCM, bahwa dari seluruh literatur yang ada belum mengintegrasikan SNI ISO/IEC 27001:2022 ke dalam kerangka hukum perlindungan data pribadi secara eksplisit. Berdasarkan analisis SLR terhadap 8 jurnal yang lolos tahap inklusi PRISMA, ditemukan bahwa seluruh studi membahas penerapan ISO/IEC 27001:2022 atau kontrol keamanan informasi sejenis dalam konteks RME di fasyankes Indonesia. Namun, tingkat kedalaman analisis serta fokus kajian menunjukkan variasi yang signifikan, khususnya dalam mengkaitkan standar keamanan informasi dengan kewajiban hukum perlindungan data pribadi. Secara umum, literatur menempatkan ISO/IEC 27001 sebagai kerangka teknis dan manajerial untuk pengelolaan keamanan informasi. Namun demikian, tidak ada satu pun studi yang secara eksplisit memposisikan SNI ISO/IEC 27001:2022 sebagai standar impelementasi SMKI atau menempatkan SNI ini sebagai instrumen normatif pendukung pemenuhan kewajiban hukum sebagaimana diatur dalam UU PDP.

Hasil dari temuan ini mengindikasikan adanya kecenderungan pemisahan antara diskursus SMKI dan analisis hukum perlindungan data pasien. SMKI masih dipahami sebagai instrumen teknis dan administratif, sementara perlindungan hak pasien dan tanggung jawab hukum fasyankes dan belum menjadi fokus utama analisis. Kondisi ini menguatkan *research gap* normatif bahwa kepatuhan terhadap ISO/IEC 27001:2022 tidak secara otomatis diterjemahkan sebagai pemenuhan kewajiban hukum berdasarkan UU PDP. Oleh karena itu, diperlukan kajian normatif berbasis sintesis sistematis. Berdasarkan dimensi teori (*theory*), hampir seluruh studi menggunakan kerangka *Confidentiality, Integrity, and Availability* (CIA *Triad*), manajemen risiko, dan tata kelola keamanan informasi berbasis standar internasional.

ISO/IEC 27001:2022 diperlakukan sebagai *best practice* secara teknis untuk mengamankan sistem RME dan mencegah terjadinya kebocoran data. Tidak ditemukan adanya penggunaan teori hukum perlindungan data pribadi, teori tanggung jawab hukum pengendali data, maupun pendekatan *rights-based* dalam menganalisis perlindungan data pasien. Hasil studi literatur cenderung

melihat keamanan data sebagai isu kepatuhan teknis organisasi, bukan sebagai bagian dari pemenuhan kewajiban hukum dan perlindungan hak subjek data. Berdasarkan hal tersebut, maka temuan ini menegaskan kekosongan konseptual dalam menjembatani teori keamanan informasi dan teori hukum perlindungan data pribadi.

Berdasarkan dimensi konteks (*context*), seluruh studi beroperasi dalam lingkungan fasyankes di Indonesia, terutama rumah sakit yang telah atau sedang dalam tahap menerapkan sistem RME. Beberapa penelitian menyebutkan regulasi sektor kesehatan dan isu privasi sebagai latar belakang, tetapi analisis tidak berkembang pada evaluasi bagaimana rezim hukum nasional yaitu pasca UU PDP dapat mempengaruhi atau tidak dalam implementasi SNI ISO/IEC 27001:2022. Dari sisi konteks hukum nasional, SNI ISO/IEC 27001:2022 secara umum diperlakukan sebagai faktor eksternal, bukan sebagai kerangka normatif utama yang menuntut penyesuaian pada implementasi SMKI. Hal ini menunjukkan bahwa konteks hukum belum diinternalisasi secara substantif dalam praktik penerapan standar di sektor kesehatan.

Tabel 1. Hasil Kajian Literatur Sistematik menggunakan TCCM *framework*

Dimensi TCCM	Sintesis Temuan (n = 8)	Dokumen Penunjang	Kesenjangan Penelitian Hukum Normatif
Theory	Dominan menggunakan kerangka CIA Triad (*Confidentiality, Integrity, Availability*), *risk management*, dan *information security governance*. ISO/IEC 27001 diposisikan sebagai *best practice* teknis, bukan sebagai instrumen normatif pendukung kewajiban hukum perlindungan data pribadi.	Permana dan Nuraeni; Ramadhan et al.; Amalia et al.	Belum ada konstruksi teoretis yang memosisikan SNI ISO/IEC 27001:2022 sebagai instrumen *due diligence* hukum dalam pemenuhan UU PDP dan perlindungan hak privasi pasien.
Context	Seluruh studi berfokus pada fasyankes di Indonesia (rumah sakit). Regulasi (PerMenKes, isu privasi) sering disebut sebagai latar belakang, tetapi UU PDP belum menjadi bingkai analisis utama.	Mubarak et al.; Widjaja dan Yustanti; Siregar dan Mardiah; Rani dan Widyaningrum.	Kesenjangan pemetaan antara konteks hukum nasional pasca UU PDP dan praktik penerapan SMKI di fasyankes.
Characteristics	Implementasi ISO/IEC 27001:2022 dicirikan oleh RBAC, kebijakan keamanan tertulis, *audit log, backup*, dan SOP insiden. Terdapat kelemahan signifikan: tidak adanya MFA, audit eksternal terbatas, dokumentasi insiden lemah, evaluasi akses tidak rutin.	Permana dan Nuraeni; Ramadhan et al.; Amalia et al.	Studi belum menilai apakah karakteristik implementasi tersebut memenuhi prinsip akuntabilitas dan kehati-hatian hukum sebagaimana disyaratkan UU PDP.
Methodology	Didominasi studi kasus tunggal, *gap analysis*, dan pendekatan deskriptif berbasis checklist ISO. Hampir tidak ditemukan analisis hukum normatif terintegrasi.	Permana dan Nuraeni; Ramadhan et al.; Amalia et al.; Mubarak et al.; Widjaja dan Yustanti; Siregar dan Mardiah; Rani dan Widyaningrum.	Belum ada sintesis sistematis yang mengevaluasi peran SNI ISO/IEC 27001:2022 sebagai instrumen normatif pendukung kewajiban hukum pengendali data.

Sumber: hasil elaborasi peneliti, 2026.

Berdasarkan dimensi karakteristik (*characteristic*), implementasi terhadap ISO/IEC 27001:2022 yang ditemukan dalam kajian literatur sistematik ini relatif seragam. Temuan meliputi penerapan *role-based access control* (RBAC), kebijakan keamanan

informasi tertulis, pencatatan *audit log*, mekanisme *backup*, dan prosedur penanganan insiden. Meskipun demikian, hampir seluruh studi juga mengidentifikasi terdapat beberapa kelemahan signifikan. Temuan tersebut seperti tidak diterapkannya *multi-factor authentication* (MFA), lemahnya dokumentasi insiden, keterbatasan audit eksternal, dan tidak rutinnya evaluasi hak akses pengguna. Karakteristik ini menunjukkan bahwa implementasi standar masih berada pada tingkat kepatuhan prosedural, belum mencapai perlindungan substantif yang dapat menjamin terpenuhinya prinsip akuntabilitas dan kehati-hatian hukum (*due diligence*) yang dituntut oleh UU PDP.

Berdasarkan dimensi metodologi (*methodology*), hasil kajian literatur sistematik ini didominasi oleh studi kasus tunggal, pendekatan deskriptif, dan *gap analysis* berbasis daftar periksa (*checklist*) ISO/IEC 27001:2022. Tidak ditemukan pendekatan sistematis untuk mengevaluasi posisi SMKI dalam konteks kewajiban hukum perlindungan data. Keterbatasan metodologis ini menyebabkan tidak adanya gambaran utuh mengenai bagaimana literatur yang ada memposisikan hubungan antara kepatuhan SMKI dan tanggung jawab hukum sebuah fasyankes.

Secara umum, hasil kajian literatur sistematik menunjukkan bahwa standar internasional ISO/IEC 27001:2022, termasuk SNI ISO/IEC 27001:2022 dipahami sebagai instrumen teknis dan manajerial, bukan sebagai *legal compliance instrument*. Padahal, dalam konteks Indonesia pasca UU PDP, penerapan standar keamanan informasi memiliki implikasi normatif yang signifikan terhadap pemenuhan kewajiban hukum pengendali data. Ketika fasyankes mengelola RME, mereka tidak hanya menghadapi risiko operasional, tetapi juga risiko tanggung jawab hukum administratif, perdata, dan bahkan pidana apabila terjadi pelanggaran data. Terdapat kesenjangan antara kepatuhan teknis dan akuntabilitas hukum. Hasil kajian literatur sistematik ini menunjukkan bahwa organisasi dapat dinyatakan '*patuh*' (*compliance*) terhadap kontrol pada standar tertentu, tetapi tetap rentan terhadap pelanggaran data yang berimplikasi hukum serius.

Kondisi-kondisi tersebut menegaskan bahwa kepatuhan terhadap SNI ISO/IEC 27001:2022 tidak bersifat *legal safe harbour*, yaitu tidak secara otomatis membebaskan fasyankes dari tanggung jawab hukum apabila hak privasi pasien dilanggar. Penerapan standar keamanan informasi juga belum dipahami sebagai kewajiban yang bersifat komplementer terhadap norma hukum, dan bersifat bukan substitusi dari kewajiban hukum itu sendiri. Temuan juga menunjukkan bahwa perlindungan data pasien masih diposisikan sebagai masalah sistem dan organisasi, bukan sebagai perlindungan hak subjek data. Perspektif hukum normatif menuntut pergeseran paradigma, dari *organization-centered compliance* menuju *patient-centered data protection*. Dalam konteks ini, efektivitas SNI ISO/IEC 27001:2022 kemudian harus diukur bukan hanya dari keberadaan kebijakan dan kontrol, tetapi dari sejauh mana standar tersebut berkontribusi pada perlindungan hak pasien atas privasi, keamanan, dan kendali atas data pribadinya.

Implikasi terhadap hukum administrasi yaitu UU PDP memberikan kewenangan kepada otoritas pengawas untuk menjatuhkan sanksi administratif kepada pengendali data yang tidak memenuhi kewajiban perlindungan data pribadi. Sanksi tersebut meliputi teguran tertulis, penghentian sementara pemrosesan data, penghapusan atau pemusnahan data pribadi, hingga denda administratif dengan persentase tertentu dari pendapatan tahunan organisasi. Temuan dari kajian literatur sistematik ini menunjukkan bahwa sebagian besar fasyankes masih berfokus pada pemenuhan persyaratan teknis dan dokumentasi ISO/IEC 27001:2022, tetapi belum mengintegrasikan standar tersebut secara penuh ke dalam tata kelola kepatuhan hukum. Ketidaksesuaian ini berpotensi mengakibatkan sanksi administratif meskipun organisasi telah menerapkan SMKI secara formal. Penerapan SNI ISO/IEC 27001:2022 hanya relevan secara administratif apabila dapat dibuktikan bahwa standar tersebut diimplementasikan secara efektif dan berkesinambungan untuk memenuhi prinsip akuntabilitas dan pencegahan pelanggaran data sebagaimana diwajibkan UU PDP.

Dalam perspektif hukum perdata, kondisi tersebut dapat menimbulkan potensi tanggung jawab ganti kerugian (*civil liability*) apabila terjadi pelanggaran data yang merugikan subjek data pasien. UU PDP pun menegaskan bahwa pengendali data pribadi bertanggung jawab atas kerugian yang

ditimbulkan akibat kegagalan melindungi data pribadi, baik akibat kesengajaan maupun kelalaian. Kepemilikan sertifikasi atau klaim penerapan ISO/IEC 27001:2022 tidak serta merta menghapus tanggung jawab perdata. Hasil kajian literatur sistematik ini menunjukkan bahwa kelemahan implementasi seperti tidak diterapkannya MFA, lemahnya dokumentasi, dan tidak rutinnya evaluasi hak akses dapat berpotensi dikualifikasikan sebagai kelalaian (*negligence*) dalam memenuhi kewajiban kehati-hatian hukum (*due diligence*). Dengan demikian, SNI ISO/IEC 27001:2022 hanya dapat berfungsi sebagai alat pembuktian upaya pengendalian risiko (*due diligence evidence*), bukan sebagai pembelaan absolut terhadap tuntutan ganti rugi perdata dari pasien sebagai subjek data.

UU PDP pun mengatur sanksi pidana terhadap perbuatan tertentu terhadap data pribadi, seperti pengumpulan, penggunaan, pengungkapan, atau pemalsuan data pribadi dapat dikatakan melawan hukum atau dikenal dengan perbuatan melanggar hukum (PMH). Meskipun ketentuan pidana tersebut mensyaratkan unsur kesengajaan atau kelalaian berat, hasil kajian literatur sistematik ini menunjukkan adanya potensi paparan pidana terhadap korporasi apabila kegagalan SMKI disebabkan oleh pembiaran struktural atau pengabaian kewajiban pengendalian risiko. Beberapa temuan ditujukkan seperti adanya kelemahan pengelolaan akses, dokumentasi insiden, dan kesadaran SDM yang dapat menjadi dasar penilaian adanya *corporate fault* atau tanggung jawab pidana korporasi (BSSN, 2023). Kondisi ini khususnya apabila pelanggaran data menimbulkan dampak luas terhadap hak privat pasien. Dalam konteks tujuan penelitian ini, penerapan SNI ISO/IEC 27001:2022 tidak serta merta berfungsi sebagai perisai pidana. Sebaliknya, kegagalan menerapkan kontrol penting yang telah diakui dalam standar justru dapat memperkuat argumen bahwa pengendali data mengetahui atau patut mengetahui risiko, tetapi tidak mengambil langkah memadai untuk mencegahnya.

SIMPULAN

Penerapan SNI ISO/IEC 27001:2022 pada fasyankes di Indonesia belum sepenuhnya berfungsi sebagai instrumen pendukung pemenuhan kewajiban hukum perlindungan data pribadi pada RME. Standar tersebut masih dipahami dan diterapkan terutama dalam kerangka kepatuhan teknis dan administratif, sehingga belum menjamin perlindungan substantif terhadap hak privasi pasien sebagaimana diwajibkan oleh Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Kepatuhan terhadap SNI ISO/IEC 27001:2022 tidak dapat diposisikan sebagai *legal safe harbour*, melainkan hanya sebagai bagian dari pembuktian *due diligence* yang harus diintegrasikan dengan tata kelola kepatuhan hukum dan pendekatan perlindungan data yang berorientasi pada hak pasien. Integrasi tersebut menegaskan bahwa efektivitas penerapan standar SMKI di sektor kesehatan hanya dapat dicapai apabila selaras dengan akuntabilitas hukum dan prinsip perlindungan data pribadi secara menyeluruh.

UCAPAN TERIMAKASIH

Ucapan terima kasih kepada Program Studi Magister Kesehatan Masyarakat, Fakultas Kesehatan Masyarakat, Universitas Hang Tuah Pekanbaru untuk penyediaan dana penelitian ini. Juga diberikan kepada Program Studi Magister Kesehatan Masyarakat, Fakultas Ilmu dan Teknologi Kesehatan (FITKes) Universitas Jenderal Achmad Yani, dan kepada rekan sejawat Justicia Medica 5, Magister Hukum Kesehatan, Pascasarjana, Universitas Udayana.

DAFTAR PUSTAKA

Kementerian Kesehatan Republik Indonesia. (2022). *Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 Tentang Rekam Medis*. Jakarta.

Kementerian Kesehatan Republik Indonesia. (2023). *Surat Edaran Nomor HK.02.01/MENKES/1030/2023 Tentang Penyelenggaraan Rekam Medis Elektronik di Fasilitas Pelayanan Kesehatan serta Penerapan Sanksi Administratif Dalam Rangka Pembinaan dan Pengawasan*. Jakarta.

Kementerian Kesehatan Republik Indonesia. (2025). Surat Edaran RS.01.04/D/6199/2025 Tentang *Penyampaian Daftar Rumah Sakit yang Belum Mengimplementasikan RME cecara Lengkap dan Belum Terintegrasi dengan Platform SATUSEHAT*. Jakarta.

Kementerian Kesehatan Republik Indonesia. (2026). *Surat Edaran Nomor YM.02.02/D/971/2026 Tentang Pemberian Sanksi Terhadap Penyelenggaraan Rekam Medis Elektronik di Rumah Sakit*. Jakarta.

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

World Health Organization. (2021). *Ethics and Governance of Health Data*. WHO Press.

Badan Standardisasi Nasional (BSN). (2023). *SNI ISO/IEC 27001:2022 Keamanan Informasi, Keamanan Siber, dan Proteksi Privasi - Sistem Manajemen Keamanan Informasi – Persyaratan (ISO/IEC 27001:2022, IDT)*. BSN.

ISO/IEC. (2022). *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements*. International Organization for Standardization.

Permana, O., & Ayu Nuraeni, Y. (2025). Evaluation of Data Security and Patient Confidentiality in the Electronic Medical Record System at Santosa Hospital Bandung Central. *Dinasti Health and Pharmacy Science*, *3*(1), 34-40. https://doi.org/10.38035/dhps.v3i1.2805

Siregar, M. N. H, & Mardiah. (2025). Analisis Keamanan Data pada Sistem Informasi Menggunakan Metode ISO/IEC 27001. (2025). *Jurnal Ilmu Komputer Dan Teknik Informatika*, *1*(2), 58-64. https://doi.org/10.64803/juikti.v1i2.52

Mubarak, H., Wiradirja, I. R., & Pranadita, N. (2025). Penegakan Hukum Terhadap Tanggungjawab Rumah Sakit Pada Pengelolaan Privasi Dan Keamanan Rekam Medis Elektronik Dalam Perspektif Hukum Progresif Di Indonesia. *Iustitia Omnibus: Jurnal Ilmu Hukum*, *6*(2), 69-76. https://jurnal-pasca.unla.ac.id/iustitiaomnibus/article/view/188

Rani, D. M., & Widyaningrum, B. N. (2025). Edukasi Peningkatan Pemahaman Keamanan Data Pasien Pada RME bagi Perekam Medis di UPTD Puskesmas Pegandon berdasarkan Permenkes Nomor 24 Tahun 2022. *Indonesian Journal of Health Information Management Services*, *5*(1), 36-41. https://doi.org/10.33560/ijhims.v5i1.133

Widjaja, G., & Ersita Yustanti, D. (2025). Tanggung Jawab Hukum Rumah Sakit di Era Digitalisasi Pelayanan Kesehatan. *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan*, *4*(10), 3517-3526. https://doi.org/10.54443/sibatik.v4i10.3642

Amalia, R., Kasmiati, N., Yorismanto, Y., Hartono, B., & Daut, A. G. (2025). Etika dalam Penggunaan Jaringan untuk Sistem Informasi Rumah Sakit. *RIGGS: Journal of Artificial Intelligence and Digital Business*, *4*(2), 5262-5268. https://doi.org/10.31004/riggs.v4i2.1419

Ramadhan, R., Widiyasono, N., & Rahmatullah, A. (2025). Evaluasi Keamanan Informasi Sistem Informasi Manajemen RSUD KHZ Musthafa Menggunakan Indeks KAMI 5.0 Berbasis ISO/IEC 27001:2022. *JoMMiT: Jurnal Multi Media dan IT*, *9*(1), 080-086. https://doi.org/10.46961/jommit.v9i1.1706

Badan Siber dan Sandi Negara (BSSN). (2023). *Urgensi Struktur Organisasi Keamanan Informasi pada Sektor Kesehatan*. Direktorat Proteksi Infrastruktur Informasi Kritis Nasional (IIKN). https://iptek.web.id/wp-content/uploads/2023/11/Artikel-Urgensi-Struktur-Organisasi-Keamanan-Informasi-pada-Sektor-Kesehatan-sign.pdf