selat media

Keamanan dan Kerahasiaan Data dalam Sistem Kesehatan

Editor :
Sri Lestari, SKM, M. Kes.

KEAMANAN DAN KERAHASIAAN DATA DALAM SISTEM KESEHATAN

Sri Lestari, S.K.M., M.Kes., dkk.

Editor: Sri Lestari, S.K.M., M.Kes.

SELAT MEDIA
Conects Your Ideas

KEAMANAN DAN KERAHASIAAN DATA DALAM SISTEM KESEHATAN

Penulis : Sri Lestari, S.K.M., M.Kes. Indah Naryanti, S.K.M., M.K.M., Arief Azhari Ilyas, A.Md.RMIK., S.St., M.K.M. Natalia Kristiani, A.Md., S.K.M., M.K.M. Setya Wijayanta, S.T., M.Kes. Praditya Dewi Arumsari, S.E., M.Si. Dyah Ayu Puspitaningtyas, M.Tr.ID. Rudiansyah, S.K.M., M.Kes., Edi Sugiarto, S.K.M., M.Kes. Muhammad Rifqi Aufa Daffa, A.Md.Kes.

Editor : Sri Lestari, S.K.M., M.Kes.
ISBN : 978-634-7465-83-2 (PDF)
Tata Letak : Selat Media Patners
Desain Sampul : Novikean Keysah Sanisri

Tebal : xi romawi + 216 halaman
Ukuran : 16 x 23 cm

Cetakan 1

Yogyakarta, Juni 2026

Diterbitkan oleh:

Penerbit Selat Media Patners
Anggota IKAPI No. 165/DIY/2022
Kertopaten RT.02 Wirokerten, Banguntapan Bantul Yogyakarta

Mitra Penerbit: **Penerbit PT Bukuloka Literasi Bangsa**
Kompleks Business Park Kebon Jeruk Blok I No. 21, Jl. Meruya Ilir Raya No. 88, Meruya Utara, Kec. Kembangan, Kota Jakarta Barat, DKI Jakarta 11620

KATA PENGANTAR

Perkembangan teknologi informasi telah membawa perubahan besar dalam tata kelola data di sektor kesehatan. Rekam medis elektronik, sistem klaim digital, dan pertukaran data antarfasilitas kesehatan kini menjadi bagian tak terpisahkan dari pelayanan kesehatan modern. Di sisi lain, transformasi digital ini menghadirkan tantangan serius terkait keamanan dan kerahasiaan data pasien yang bersifat sangat sensitif. Ancaman siber yang terus berkembang, kerentanan sistem, serta kebutuhan akan kepatuhan terhadap regulasi perlindungan data menjadikan pemahaman mengenai keamanan data kesehatan sebagai kompetensi yang wajib dimiliki oleh seluruh pihak yang terlibat dalam ekosistem kesehatan.

Buku ini disusun untuk memberikan pemahaman yang komprehensif mengenai prinsip, regulasi, teknologi, dan praktik terbaik dalam menjaga keamanan dan kerahasiaan data di lingkungan sistem kesehatan. Pembahasan dimulai dari konsep dasar keamanan data dan rekam medis, dilanjutkan dengan prinsip-prinsip keamanan informasi, identifikasi ancaman dan kerentanan, perlindungan data dalam sistem informasi kesehatan, keamanan data pada pembiayaan kesehatan, hak akses dan privasi pasien, audit dan pengawasan, hingga penanganan insiden kebocoran data. Setiap bab dilengkapi dengan latihan soal untuk memperdalam pemahaman pembaca terhadap materi yang dibahas.

Penulis menyadari bahwa buku ini masih memiliki keterbatasan dan memerlukan penyempurnaan. Oleh karena itu,

kritik dan saran yang membangun dari pembaca sangat diharapkan demi perbaikan pada edisi berikutnya. Semoga buku ini dapat menjadi referensi yang bermanfaat bagi mahasiswa, tenaga kesehatan, pengelola sistem informasi kesehatan, serta siapa pun yang ingin memahami pentingnya menjaga keamanan dan kerahasiaan data dalam sistem kesehatan.

Yogyakarta, Juni 2026

Tim Penulis

DAFTAR ISI

BAB 1
PENGANTAR KEAMANAN DAN KERAHASIAAN DATA KESEHATAN

Sri Lestari, SKM, M. Kes

1.1 Definisi dan Pentingnya Keamanan Data Kesehatan

1.1.1 Konsep Dasar Keamanan Data Kesehatan

Keamanan data kesehatan merupakan aspek fundamental dalam sistem informasi kesehatan modern yang dirancang untuk melindungi informasi sensitif pasien dari akses tidak sah, modifikasi, atau kehancuran. Dalam era digitalisasi yang pesat, data kesehatan telah berkembang dari catatan berbasis kertas menjadi rekam medis elektronik atau *electronic health records* (EHR) yang tersimpan dalam sistem informasi berbasis komputer. Perubahan paradigma ini membawa konsekuensi serius terhadap kebutuhan akan mekanisme keamanan yang lebih canggih dan terstruktur (Rajeswari & Chakravarthy, 2026). Data kesehatan mencakup informasi pribadi pasien seperti identitas, riwayat medis, hasil laboratorium, resep obat, dan informasi finansial kesehatan yang semuanya termasuk dalam kategori data sensitif dengan nilai tinggi di pasar gelap siber (Musale et al., 2025).

Keamanan data kesehatan bukan hanya tentang teknologi enkripsi atau sistem pertahanan jaringan, tetapi juga melibatkan aspek administratif, fisik, dan legal yang saling terintegrasi. Sistem keamanan yang komprehensif harus mencakup kebijakan organisasi yang jelas, prosedur operasional standar, pelatihan karyawan, teknologi enkripsi terkini, kontrol akses yang ketat, serta mekanisme audit dan pemantauan berkelanjutan (Javeedullah, 2025). Organisasi kesehatan yang modern harus mengakui bahwa keamanan data bukan biaya tambahan atau tugas yang dapat ditangguhkan, melainkan investasi strategis yang sangat diperlukan untuk mempertahankan kepercayaan pasien dan memenuhi kewajiban hukum (A & Prasanna, 2024).

1.1.2 Dimensi Keamanan: Confidentiality, Integrity, dan Availability

Keamanan data kesehatan dibangun atas tiga pilar fundamental yang dikenal dengan singkatan CIA, yaitu Confidentiality (Kerahasiaan), *Integrity* (Integritas), dan Availability (Ketersediaan). Konsep ini menjadi dasar dalam perlindungan rekam medis sebagaimana ditegaskan dalam berbagai regulasi nasional seperti Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis.

Confidentiality atau kerahasiaan berarti bahwa hanya pihak yang berwenang saja yang dapat mengakses informasi kesehatan

pasien. Kerahasiaan adalah prinsip bahwa informasi kesehatan pasien hanya dapat diakses oleh pihak yang berwenang dan memiliki kepentingan sesuai tugas profesionalnya.

Menurut Hatta (2013) dalam *Manajemen Informasi Kesehatan di Sarana Pelayanan Kesehatan*, rekam medis mengandung data pribadi yang bersifat rahasia dan wajib dijaga oleh seluruh tenaga kesehatan maupun tenaga rekam medis sebagai bentuk perlindungan hak pasien.

Sementara itu, menurut Siswati (2017) dalam kajian hukum kesehatan, kerahasiaan rekam medis merupakan bagian dari perlindungan hak asasi pasien atas privasi.

Prinsip ini sangat penting mengingat data kesehatan adalah informasi yang sangat pribadi dan sensitif, di mana pengungkapan tanpa izin dapat menyebabkan kerugian reputasi, diskriminasi, atau kerugian finansial bagi pasien (Kumar, 2025). Teknologi enkripsi berbasis *Advanced Encryption Standard* (AES) dan *Elliptic Curve Cryptography* (ECC) telah terbukti efektif dalam menjaga kerahasiaan data dalam sistem komunikasi kesehatan (Musale et al., 2025).

Integrity atau integritas mengacu pada jaminan bahwa data kesehatan tidak mengalami modifikasi, penghapusan, atau kerusakan baik secara sengaja maupun tidak sengaja. Integritas memiliki makna bahwa data kesehatan harus akurat, lengkap, konsisten dan tidak dimodifikasi secara tidak sah. Dalam konteks medis, integritas data sangat kritis karena informasi yang tidak

akurat atau telah diubah dapat membahayakan nyawa pasien dan menghasilkan keputusan klinis yang salah (Wang & Sun, 2024). Mekanisme pendeteksian perubahan seperti digital signature dan *hash function* digunakan untuk memastikan bahwa setiap data yang dikirim atau disimpan tetap dalam kondisi original dan belum mengalami modifikasi. Dengan mengintegrasikan teknologi *Blockchain*, sistem dapat menciptakan jejak audit yang tidak dapat diubah dan memastikan transparansi penuh dalam setiap transaksi data kesehatan (Vidhya et al., 2024). Budi (2011) dalam literatur sistem informasi kesehatan, menyatakan integritas data sangat menentukan kualitas pelayanan karena keputusan klinis bergantung pada keakuratan informasi pasien.

Availability atau ketersediaan memastikan bahwa data dan sistem informasi kesehatan selalu dapat diakses oleh pihak yang berwenang pada saat dibutuhkan, untuk kepentingan pelayanan, hukum, maupun administrasi. Sabarguna (2008) menjelaskan , sistem informasi rumah sakit harus menjamin kontinuitas pelayanan melalui ketersediaan data yang cepat dan tepat.Dalam situasi darurat medis, sistem yang mengalami downtime atau tidak responsif dapat berakibat fatal bagi pasien. Ketersediaan sangat penting dalam kondisi gawat darurat, karena keterlambatan akses data dapat berdampak langsung pada keselamatan pasien. Oleh karena itu, organisasi kesehatan harus mengimplementasikan mekanisme backup, *disaster recovery*, dan redundansi sistem untuk memastikan kontinuitas layanan (A & Prasanna, 2024). Pertumbuhan adopsi

cloud computing dalam sektor kesehatan menuntut bahwa penyedia layanan cloud harus menjamin waktu aktif sistem (*uptime*) mencapai level Service Level Agreement (SLA) yang tinggi, umumnya di atas 99.9% (Kurra, 2025).

1.1.3 Perbedaan Antara Privacy dan Security

Meskipun sering digunakan secara bergantian, konsep *privacy* dan *security* memiliki perbedaan mendasar dalam konteks data kesehatan. *Privacy* atau kerahasiaan adalah hak fundamental individu untuk mengontrol informasi pribadi mereka, termasuk bagaimana data dikumpulkan, digunakan, dibagikan, dan disimpan. Prinsip *privacy* berfokus pada otonomi dan kontrol individu atas data pribadi mereka, sementara *security* adalah mekanisme teknis dan administratif yang digunakan untuk melindungi data tersebut dari akses tidak sah atau ancaman keamanan (Smit et al., 2022). Regulasi global seperti *General Data Protection Regulation* (GDPR) di Eropa dan *Health Insurance Portability and Accountability Act* (HIPAA) di Amerika Serikat mencerminkan komitmen untuk melindungi privasi data kesehatan dengan menetapkan standar keamanan yang ketat (Shah, 2023).

Organisasi kesehatan harus memahami bahwa melindungi privasi pasien bukan hanya tentang mengimplementasikan teknologi enkripsi, tetapi juga tentang menciptakan budaya organisasi yang menghormati hak privasi individu. Hal ini mencakup transparansi dalam pengumpulan dan penggunaan data, mendapatkan persetujuan (*informed consent*) yang jelas dari pasien, serta memberikan kepada

pasien hak untuk mengakses dan mengubah data mereka sendiri (Javeedullah, 2025). Dalam praktiknya, banyak organisasi kesehatan masih belum sepenuhnya memahami perbedaan ini dan cenderung fokus pada aspek keamanan teknis sambil mengabaikan dimensi privasi yang lebih luas (Amri et al., 2024).

1.1.4 Risiko dan Dampak Pelanggaran Data Kesehatan

Pelanggaran data kesehatan memiliki konsekuensi yang jauh lebih parah dibandingkan dengan sektor industri lainnya. Ketika informasi sensitif pasien seperti diagnosis, riwayat penyakit, atau data genetik bocor, dampak dapat mencakup dampak fisik, emosional, finansial, dan sosial yang signifikan bagi pasien (Amri et al., 2024). Untuk contoh, penyalahgunaan data kesehatan dapat menyebabkan diskriminasi dalam pekerjaan, pengasuransian, atau bahkan perawatan medis di masa depan. Selain itu, pencurian identitas medis dapat mengakibatkan pengguna yang tidak sah melakukan prosedur medis atau klaim asuransi atas nama pasien yang sebenarnya (Kumar, 2025).

Dari perspektif organisasi, pelanggaran data kesehatan dapat berakibat pada kerugian finansial yang sangat besar. Regulasi seperti HIPAA di Amerika Serikat mengenakan denda yang dapat mencapai jutaan dolar untuk setiap pelanggaran, sementara GDPR di Eropa mengenakan denda hingga 4% dari pendapatan tahunan global organisasi atau 20 juta Euro, mana pun yang lebih besar (Abbasi & Smith, 2024). Selain denda regulasi, organisasi juga menghadapi kehilangan reputasi, penurunan kepercayaan pasien, dan biaya

remediasi yang signifikan. Survei menunjukkan bahwa biaya rata-rata pemulihan dari pelanggaran data kesehatan mencapai jutaan dolar per organisasi, termasuk biaya notifikasi, legal, investigasi, dan peningkatan keamanan (A & Prasanna, 2024).

1.2 Lanskap Regulasi Global untuk Data Kesehatan

1.2.1 Regulasi Eropa: General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) yang mulai berlaku sejak Mei 2018 di Uni Eropa telah mengubah lanskap perlindungan data secara fundamental. GDPR adalah regulasi yang paling komprehensif dan ketat di dunia dalam hal perlindungan data pribadi, termasuk data kesehatan yang dikategorikan sebagai data sensitif khusus (Shah, 2023). Regulasi ini menetapkan prinsip-prinsip dasar yang harus diikuti oleh semua organisasi yang memproses data pribadi dari individu di Uni Eropa, terlepas dari lokasi geografis organisasi tersebut (Vw et al., 2024).

Beberapa prinsip inti GDPR yang relevan dengan data kesehatan mencakup prinsip *lawfulness, fairness, and transparency*, yang berarti organisasi harus memiliki dasar hukum yang jelas untuk memproses data dan harus transparan kepada individu tentang bagaimana data mereka digunakan. GDPR juga menetapkan prinsip *purpose limitation* yang berarti data hanya dapat digunakan untuk tujuan tertentu yang telah dinyatakan kepada individu, dan tidak dapat digunakan untuk tujuan lain tanpa persetujuan baru.

Prinsip *data minimization* menyatakan bahwa organisasi hanya boleh mengumpulkan dan memproses data yang benar-benar diperlukan untuk mencapai tujuan yang telah dinyatakan (Zadavul, 2024). Implementasi GDPR di organisasi kesehatan memerlukan perubahan signifikan dalam bagaimana data dikumpulkan, diproses, disimpan, dan dibagikan.

Hak-hak individu yang dijamin oleh GDPR termasuk hak akses (*right of access*), hak untuk dihapus atau dilupakan (*right to be forgotten*), hak untuk keberatan (*right to object*), dan hak untuk portabilitas data (*right to data portability*). Hak untuk dilupakan memungkinkan individu untuk meminta penghapusan data pribadi mereka dalam kondisi tertentu, yang dapat menjadi tantangan dalam sektor kesehatan di mana data mungkin perlu dipertahankan untuk keperluan medis jangka panjang (Smit et al., 2022). Organisasi kesehatan harus mengembangkan kebijakan dan prosedur yang jelas untuk menangani permintaan ini tanpa mengorbankan aspek keamanan data atau kepatuhan regulasi lainnya (Zadavul, 2024).

1.2.2 Regulasi Amerika Serikat: HIPAA dan HITECH Act

Di Amerika Serikat, perlindungan data kesehatan terutama diatur oleh *Health Insurance Portability and Accountability Act* (HIPAA) yang diberlakukan pada tahun 1996, kemudian diperkuat oleh *Health Information Technology for Economic and Clinical Health* (HITECH) Act pada tahun 2009 (Abbasi & Smith, 2024). HIPAA menetapkan standar nasional untuk melindungan informasi kesehatan pribadi yang dikenal sebagai *Protected Health*

Information (PHI), yang mencakup semua informasi dalam rekam medis atau informasi kesehatan yang dapat diidentifikasi dengan individu tertentu (Osifowokan et al., 2025).

HIPAA membagi persyaratan kepatuhan menjadi tiga kategori utama: *Administrative Safeguards*, *Physical Safeguards*, dan *Technical Safeguards*. *Administrative Safeguards* meliputi kebijakan dan prosedur organisasi, manajemen akses pengguna, pelatihan karyawan, manajemen insiden keamanan, dan audit berkelanjutan. *Physical Safeguards* mencakup kontrol akses fisik terhadap fasilitas dan perangkat di mana PHI disimpan atau diproses, termasuk penggunaan kartu akses, video surveillance, dan penguncian area sensitif. *Technical Safeguards* meliputi enkripsi data, kontrol akses berbasis teknologi, logging dan monitoring sistem, dan manajemen vulnerabilitas (Osifowokan et al., 2025).

HITECH Act memperkuat HIPAA dengan menetapkan persyaratan keamanan yang lebih ketat, termasuk persyaratan untuk notifikasi pelanggaran, investigasi insiden keamanan, dan dokumentasi audit yang komprehensif. HITECH juga memperluas definisi "pelanggaran" (*breach*) untuk mencakup situasi di mana akses tidak sah atau pengungkapan yang tidak disengaja terjadi pada PHI (Abbasi & Smith, 2024). Penyedia layanan kesehatan di Amerika Serikat harus melakukan penilaian risiko berkelanjutan, mengimplementasikan rencana manajemen risiko, dan memastikan bahwa semua staf yang menangani data kesehatan menerima pelatihan keamanan data yang memadai (Jagadeesan, 2024).

1.2.3 Regulasi Regional Lainnya: POPIA, PDPA, dan Regulasi Lokal

Di luar GDPR dan HIPAA, berbagai negara dan region telah mengembangkan regulasi privasi data mereka sendiri yang juga berlaku untuk data kesehatan. *Protection of Personal Information Act* (POPIA) di Afrika Selatan mengikuti pola yang serupa dengan GDPR dalam hal perlindungan data pribadi dan menetapkan standar tinggi untuk keamanan data (Conduah et al., 2025). Di Asia, berbagai negara seperti Singapura, Thailand, dan Indonesia memiliki undang-undang perlindungan data pribadi mereka sendiri, meskipun tingkat kematangan dan implementasi bervariasi di seluruh wilayah.

Indonesia, misalnya, memiliki beberapa regulasi yang relevan termasuk Undang-Undang Nomor 29 Tahun 2008 tentang Praktik Kedokteran, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, dan Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan. Namun, penelitian menunjukkan bahwa kerangka regulasi ini masih memiliki kelemahan struktural dalam menjamin privasi data pasien dalam sistem kesehatan elektronik (Santhi, 2025). Perbedaan regulasi antara berbagai yurisdiksi menciptakan tantangan khusus bagi organisasi kesehatan multinasional yang harus memastikan kepatuhan terhadap standar yang berbeda-beda di setiap negara tempat mereka beroperasi (Vw et al., 2024).

1.2.4 Implikasi Kepatuhan Regulasi dalam Praktik Organisasi Kesehatan

Kepatuhan terhadap regulasi data kesehatan bukan hanya tentang menghindari denda regulasi, tetapi juga tentang membangun kepercayaan pasien dan menciptakan budaya organisasi yang menghormati privasi individual. Organisasi kesehatan yang gagal mematuhi persyaratan regulasi menghadapi risiko signifikan termasuk denda finansial yang besar, tuntutan hukum dari pasien yang dirugikan, kehilangan lisensi operasional, dan kerusakan reputasi yang berkelanjutan (Abbasi & Smith, 2024). Untuk mencapai kepatuhan yang efektif, organisasi harus melakukan penilaian dampak privasi yang menyeluruh, mengidentifikasi area di mana sistem dan proses saat ini tidak memenuhi persyaratan regulasi, dan mengembangkan rencana perbaikan yang jelas dengan timeline yang realistis.

Tantangan utama dalam implementasi kepatuhan regulasi mencakup kompleksitas teknis dalam mengenkripsi dan melindungi data, biaya investasi yang signifikan dalam infrastruktur keamanan baru, kebutuhan akan pelatihan karyawan yang berkelanjutan, dan tantangan dalam menyeimbangkan keamanan dengan operasionalitas sistem kesehatan sehari-hari (Samant, 2024). Banyak organisasi kesehatan, terutama yang lebih kecil atau di negara berkembang, masih berjuang untuk mencapai kepatuhan penuh terhadap standar internasional karena keterbatasan sumber daya finansial dan keahlian teknis (Vw et al., 2024). Pemerintah dan

organisasi internasional perlu memberikan dukungan yang lebih besar melalui pedoman implementasi yang lebih jelas, pendanaan untuk peningkatan infrastruktur, dan pelatihan yang lebih luas untuk para profesional kesehatan dan administrator sistem.

1.3 Teknologi dan Mekanisme Enkripsi untuk Perlindungan Data

1.3.1 Enkripsi Simetris dan Asimetris

Enkripsi merupakan salah satu teknologi fundamental dalam melindungi kerahasiaan data kesehatan. Enkripsi simetris atau *symmetric key encryption* menggunakan satu kunci yang sama untuk mengenkripsi dan mendekripsi data. *Advanced Encryption Standard* (AES) dengan panjang kunci 256-bit telah menjadi standar industri dalam enkripsi data kesehatan karena kecepatan pemrosesan dan keamanan yang tinggi (Musale et al., 2025). Keunggulan enkripsi simetris adalah kecepatan dan efisiensi komputasi yang membuatnya cocok untuk mengenkripsi jumlah data yang sangat besar, seperti basis data pasien besar yang berisi jutaan rekam medis (A & Prasanna, 2024).

Enkripsi asimetris atau *asymmetric key encryption*, di mana terdapat sepasang kunci publik dan kunci privat, menyediakan solusi untuk masalah distribusi kunci yang timbul dengan enkripsi simetris. *Elliptic Curve Cryptography* (ECC) telah menunjukkan keunggulan dibandingkan dengan sistem RSA tradisional dalam hal panjang kunci yang lebih pendek dan overhead komputasi yang lebih

rendah (Musale et al., 2025). ECC sangat relevan untuk implementasi dalam perangkat kesehatan portabel atau sistem *Internet of Medical Things* (IoMT) di mana daya pemrosesan terbatas. Kombinasi enkripsi simetris dan asimetris, yang dikenal sebagai enkripsi hybrid, memungkinkan organisasi kesehatan untuk mendapatkan manfaat dari kecepatan enkripsi simetris sambil mempertahankan keamanan distribusi kunci asimetris (Musale et al., 2025).

1.3.2 Homomorphic Encryption dan Zero-Knowledge Proof

Homomorphic Encryption (HE) adalah teknologi enkripsi canggih yang memungkinkan perhitungan dilakukan pada data terenkripsi tanpa perlu mendekripsi data terlebih dahulu. Dalam konteks data kesehatan, teknologi ini sangat berharga karena memungkinkan organisasi kesehatan untuk melakukan analisis data yang diperlukan untuk penelitian medis dan diagnosis tanpa pernah mengungkapkan data pasien yang sebenarnya (Jayaweera et al., 2025). *Fully Homomorphic Encryption* (FHE) memungkinkan jumlah perhitungan tanpa batas pada data terenkripsi, meskipun dengan overhead komputasi yang signifikan, sementara *Somewhat Homomorphic Encryption* (SWHE) membatasi jenis dan jumlah perhitungan tetapi dengan efisiensi yang lebih baik (A & Prasanna, 2024).

Zero-Knowledge Proof (ZKP) adalah protokol kriptografi yang memungkinkan satu pihak untuk membuktikan kepada pihak lain bahwa mereka memiliki pengetahuan tentang informasi tertentu

tanpa mengungkapkan informasi tersebut secara langsung. Dalam sistem keamanan data kesehatan, ZKP dapat digunakan untuk autentifikasi pasien atau penyedia layanan kesehatan tanpa perlu mengirimkan kredensial asli melalui jaringan (Musale et al., 2025). Teknologi ini sangat berguna dalam skenario di mana diperlukan verifikasi identitas atau otorisasi akses tanpa mengekspos informasi sensitif, seperti dalam sistem pertukaran data kesehatan antar organisasi (Wang & Sun, 2024).

1.3.3 *Blockchain* dan Teknologi Terdistribusi

Blockchain adalah teknologi buku besar terdistribusi yang menciptakan catatan permanen dan tidak dapat diubah dari setiap transaksi atau perubahan data. Dalam konteks data kesehatan, *Blockchain* dapat digunakan untuk membuat sistem audit trail yang tidak dapat dimanipulasi, memastikan integritas data, dan menciptakan sistem pertukaran data yang transparan antar stakeholder kesehatan (Vidhya et al., 2024). Teknologi *Blockchain* juga memungkinkan implementasi *smart contracts*, yang merupakan program otomatis yang dapat mengeksekusi persyaratan akses data berdasarkan kriteria yang telah ditetapkan sebelumnya, tanpa perlu intervensi manual (Gupta et al., 2025).

Implementasi *Blockchain* dalam sistem kesehatan dapat mencakup penggunaan untuk manajemen rekam medis elektronik, supply chain manajemen perangkat medis, manajemen consent pasien, dan sistem verifikasi sertifikat vaksinasi atau tes kesehatan. Namun, *Blockchain* juga memiliki keterbatasan termasuk

skalabilitas terbatas, kecepatan transaksi yang lambat dibandingkan dengan sistem database tradisional, dan konsumsi energi yang tinggi untuk beberapa jenis *Blockchain* (Ma & Zhang, 2024). Oleh karena itu, penggunaan *Blockchain* dalam sistem kesehatan harus dipertimbangkan dengan cermat berdasarkan kebutuhan spesifik organisasi, dan mungkin lebih cocok untuk fungsi-fungsi tertentu seperti audit trail atau verifikasi identitas daripada untuk penyimpanan data primer (Shakila et al., 2024).

1.3.4 Teknologi Keamanan Emerging: Quantum Cryptography dan Federated Learning

Quantum Cryptography mewakili generasi berikutnya dalam keamanan enkripsi data, memanfaatkan prinsip-prinsip mekanika kuantum untuk menciptakan saluran komunikasi yang sepenuhnya aman dari intersepsi (Basha et al., 2024). Quantum cryptography menggunakan foton individu untuk mengkodekan informasi dan dapat mendeteksi segala upaya untuk mengintervensi transmisi, menjadikannya sangat relevan untuk perlindungan data kesehatan yang paling sensitif sekalipun. Meskipun teknologi ini masih dalam tahap pengembangan dan implementasi komersial masih terbatas, penelitian menunjukkan potensi signifikan untuk organisasi kesehatan yang menangani data paling sensitif seperti informasi genetik atau HIV.

Federated Learning adalah paradigma pembelajaran mesin yang memungkinkan pelatihan model di data terdesentralisasi tanpa mengumpulkan semua data ke satu lokasi pusat. Dalam sistem

kesehatan, ini berarti berbagai rumah sakit atau organisasi kesehatan dapat berkolaborasi untuk melatih model prediksi kesehatan bersama sambil menjaga data pasien tetap tersimpan secara lokal (Jayaweera et al., 2025). Teknologi ini sangat relevan untuk organisasi kesehatan yang ingin berpartisipasi dalam penelitian medis kolaboratif tanpa harus berbagi data pasien yang sensitif dengan organisasi lain. Ketika dikombinasikan dengan teknologi seperti homomorphic encryption dan differential privacy, federated learning dapat memberikan tingkat privasi yang sangat tinggi sambil tetap memungkinkan analisis data yang bermakna (Tang et al., 2024).

1.4 Ancaman Keamanan dan Tantangan Implementasi

1.4.1 Jenis-Jenis Ancaman Keamanan Data Kesehatan

Ancaman terhadap data kesehatan dapat diklasifikasikan ke dalam beberapa kategori utama. Ancaman eksternal mencakup serangan dari aktor yang tidak memiliki akses sah terhadap sistem, termasuk serangan *ransomware* yang mengenkripsi data kemudian meminta pembayaran untuk mendapatkan kembali akses, serangan *malware* yang memasukkan program berbahaya ke dalam sistem, serangan *phishing* yang mencoba menipu karyawan untuk mengungkapkan kredensial akses, dan serangan *denial of service* (DoS) yang membuat sistem tidak tersedia bagi pengguna yang sah (Javeedullah, 2025). Petugas yang melakukan penyalahgunaan akses merupakan serangan internal, baik sengaja ataupun tidak penyalahgunaan akses tersebut merupakan salah satu

ancaman yang perlu diwaspadai. Serangan tersebut seringkali ditujukan khusus pada organisasi kesehatan karena nilai tinggi data kesehatan di pasar gelap dan dampak kritis dari downtime sistem pada layanan pasien (Abbasi & Smith, 2024).

Ancaman internal adalah risiko dari individu yang memiliki akses sah terhadap sistem tetapi menyalahgunakan akses mereka untuk mengakses atau mengungkapkan data pasien yang tidak diperlukan untuk pekerjaan mereka. Insiden ini dapat terjadi karena kurangnya kesadaran keamanan di antara karyawan, disgruntled employees yang ingin merugikan organisasi, atau error manusia yang tidak disengaja seperti mengirim email sensitif ke penerima yang salah (Alexander & Candiwan, 2024). Penelitian menunjukkan bahwa faktor manusia bertanggung jawab atas persentase yang signifikan dari pelanggaran data kesehatan, menunjukkan perlunya fokus yang kuat pada pelatihan keamanan dan budaya organisasi yang mendukung privasi (Alexander & Candiwan, 2024).

1.4.2 Tantangan Teknis dalam Implementasi Keamanan

Organisasi kesehatan menghadapi berbagai tantangan teknis dalam mengimplementasikan mekanisme keamanan yang efektif. Salah satu tantangan utama adalah heterogenitas sistem yang ada di lingkungan kesehatan, di mana organisasi kesehatan sering menjalankan kombinasi sistem warisan (*legacy systems*) yang dirancang puluhan tahun lalu dengan sistem modern yang berbasis cloud. Sistem-sistem ini menggunakan arsitektur, protokol, dan standar yang berbeda, sehingga sulit untuk menerapkan keamanan

konsisten di seluruh organisasi (Jagadeesan, 2024). Integrasi sistem menjadi sangat kompleks ketika terdapat kebutuhan untuk berbagi data antar sistem sambil tetap menjaga keamanan dan privasi data (Mahajan, 2025).

Tantangan lain adalah keterbatasan infrastruktur teknologi, terutama di negara-negara berkembang atau organisasi kesehatan yang lebih kecil. Banyak rumah sakit di daerah terpencil atau negara dengan sumber daya terbatas masih mengandalkan infrastruktur jaringan yang lambat dan tidak stabil, hardware yang ketinggalan zaman, dan perangkat lunak yang tidak diperbarui dengan pita keamanan terbaru (Vw et al., 2024). Memperbarui infrastruktur ini memerlukan investasi finansial yang signifikan yang mungkin tidak dapat dialokasikan oleh organisasi kesehatan yang sudah berjuang dengan keterbatasan anggaran (Osifowokan et al., 2025). Selain itu, kebutuhan akan keseimbangan antara keamanan dan usability juga menjadi tantangan, di mana sistem keamanan yang terlalu ketat dapat menghambat efisiensi kerja klinik dan mengakibatkan resistance dari staff medis (Jagadeesan, 2024).

1.4.3 Tantangan Organisasi dan Manusia

Tantangan organisasi dalam keamanan data kesehatan meluas melampaui aspek teknis. Banyak organisasi kesehatan tidak memiliki struktur organisasi yang jelas untuk mengelola keamanan data, dengan tanggung jawab yang tersebar di antara berbagai departemen tanpa koordinasi yang efektif (Osifowokan et al., 2025). Keahlian dalam keamanan data kesehatan masih langka di pasar, dan

organisasi menghadapi kesulitan dalam merekrut dan mempertahankan profesional keamanan siber yang berkualifikasi (Kan, 2024). Pelatihan keamanan yang tidak memadai atau tidak berkelanjutan juga merupakan masalah umum, di mana banyak organisasi hanya melakukan pelatihan keamanan sekali setahun daripada pelatihan berkelanjutan dan reguler (Alexander & Candiwan, 2024).

Aspek budaya organisasi juga memainkan peran penting. Jika kepemimpinan organisasi tidak membuat keamanan data sebagai prioritas strategis, akan sulit untuk mengimplementasikan program keamanan yang komprehensif dan berkelanjutan. Karyawan perlu memahami bahwa keamanan data bukan hanya tanggung jawab departemen IT, tetapi tanggung jawab bersama semua orang dalam organisasi yang menangani data kesehatan (Kayondo & Kyobe, 2025). Budaya di mana pengguna tidak takut untuk melaporkan insiden keamanan atau mengajukan pertanyaan tentang praktik keamanan adalah penting untuk membangun sistem keamanan yang efektif (Alexander & Candiwan, 2024).

1.4.4 Dampak Transformasi Digital dan Adopsi Teknologi Baru

Transformasi digital dalam sektor kesehatan, termasuk adopsi *electronic health records*, telemedicine, sistem *Internet of Medical Things*, dan analitik data berbasis cloud, telah membuka peluang baru tetapi juga menciptakan permukaan serangan yang lebih luas untuk ancaman keamanan siber (Javeedullah, 2025).

Telemedicine yang berkembang pesat, terutama selama pandemi COVID-19, memerlukan pertukaran data kesehatan melalui jaringan internet publik yang kurang aman, meningkatkan risiko intersepsi atau modifikasi data (Amri et al., 2024). *Internet of Medical Things*, yang mencakup perangkat seperti monitor detak jantung portabel, pompa insulin, dan ventilator yang terhubung ke jaringan, menambah kompleksitas keamanan karena perangkat-perangkat ini seringkali memiliki kemampuan keamanan yang terbatas dan sulit untuk diperbarui dengan patch keamanan terbaru (Si-Ahmed et al., 2024).

Teknologi kecerdasan buatan dan pembelajaran mesin, sambil menawarkan potensi besar untuk diagnosis dan prediksi penyakit yang lebih akurat, juga menghadirkan tantangan keamanan baru. Model pembelajaran mesin dapat membuat keputusan yang sulit untuk dijelaskan atau diaudit, dan dapat rentan terhadap serangan tertentu seperti *adversarial attacks* di mana data input yang sedikit dimodifikasi dapat menyebabkan model membuat prediksi yang salah (Fei et al., 2024). Perlunya melindungi privasi data pelatihan model pembelajaran mesin sambil tetap mempertahankan akurasi model adalah tantangan yang terus berlanjut dalam penelitian keamanan data kesehatan (Jayaweera et al., 2025).

Latihan Soal

1. Jelaskan perbedaan fundamental antara konsep "*privacy*" dan "*security*" dalam konteks data kesehatan, dan berikan contoh

bagaimana kedua konsep tersebut dapat bekerja bersama dalam sistem informasi kesehatan modern.

2. Diskusikan tiga pilar fundamental keamanan data kesehatan (CIA - *Confidentiality, Integrity, Availability*) dan jelaskan mengapa ketiga elemen ini sama pentingnya dalam konteks layanan kesehatan yang menyelamatkan nyawa.
3. Bandingkan dan kontraskan pendekatan regulasi GDPR (Eropa), HIPAA (Amerika Serikat), dan regulasi regional lainnya dalam melindungi data kesehatan, serta jelaskan tantangan yang dihadapi organisasi kesehatan multinasional
4. Jelaskan bagaimana kombinasi teknologi enkripsi hybrid (simetris + asimetris), *homomorphic encryption*, dan *Blockchain* dapat bekerja bersama untuk menciptakan sistem kesehatan yang aman dan sekaligus memungkinkan kolaborasi penelitian yang aman.
5. Analisis tantangan utama yang dihadapi organisasi kesehatan dalam implementasi program keamanan data yang komprehensif, dengan fokus khusus pada interaksi antara tantangan teknis, organisasi, dan manusia.

DAFTAR PUSTAKA

American College of Radiology. (2022). *GDPR controlled patient information exchange and traceability in clinical processes*. Proceedings of the IEEE International Conference on Systems, Signals and Image Processing (SETIT), 1-6.

Abid, A., Cheikhrouhou, S., Kallel, S., & Jmael, M. (2021). NovidChain: *Blockchain*-based privacy-preserving platform for COVID19 test/vaccine certificates. *Software: Practice and Experience, 51*(5), 1143-1165. **https://doi.org/10.1002/spe.2983**

Alfawzan, N., Christen, M., Spitale, G., & Biller-Andorno, N. (2022). Privacy, data sharing, and data security policies of women's mHealth apps: Scoping review and content analysis. *JMIR Mhealth and Uhealth, 10*(2), e33735. **https://doi.org/10.2196/33735**

Amri, I., Sagalane, A. B., Kurniawan, L., Julianto, A., & Ta'adi. (2024). Legal and ethical challenges in digital health data privacy: Navigating patient rights and data security in telemedicine. *Global Journal of Medicine and Medical Sciences, 2*(11), 363.

Asenso, D., Ashong, M., Baidoo, E. N., Ansah, K. A., Opoku, O., Agyemang-Duah, W., ... & Addo, A. (2025). Data privacy in healthcare: Global challenges and solutions. *SAGE Open, 15*(2),

20552076251343959. https://doi.org/10.1177/20552076251343959

Basha, C. B., Murugan, K., Suresh, T., SrirengaNachiyar, V., Athimoolam, S., & Kanmani Pappa, C. (2024). Enhancing healthcare data security using quantum cryptography for efficient and robust encryption. *Journal of Educational Studies, 2544*, 52-78. https://doi.org/10.52783/jes.2544

Chen, Z., Du, J., Hou, X., Yu, K., Wang, J., & Han, Z. (2024). Channel adaptive and sparsity personalized federated learning for privacy protection in smart healthcare systems. *IEEE Journal of Biomedical and Health Informatics, 28*(3), 1234-1245. https://doi.org/10.1109/JBHI.2024.3353791

Coronado, A. J., & Wong, T. L. U. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. *Biomedical Instrumentation & Technology, 48*(S1), 26-33. https://doi.org/10.2345/0899-8205-48.s1.26

Conduah, A. K., Ofoe, S. H., & Siaw-Marfo, D. (2025). Data privacy in healthcare: Global challenges and solutions. *SAGE Open Medicine, 13*, 20552076251343959. https://doi.org/10.1177/20552076251343959

Fei, X., Chai, S., He, W., Dai, L., Xu, R., & Cai, L. (2024). A systematic study on the privacy protection mechanism of natural language processing in medical health

records. *Proceedings of IEEE International Conference on Sensor Networks and Signal Processing, 1-7*. **https://doi.org/10.1109**

Budi, S. C. (2011). *Manajemen Unit Kerja Rekam Medis*. Yogyakarta: Quantum Sinergis Media.

Hatta, G. (2013). *Manajemen Informasi Kesehatan di Sarana Pelayanan Kesehatan*. Jakarta: UI Press.

Sabarguna, B. S. (2008). *Sistem Informasi Manajemen Rumah Sakit*. Yogyakarta: Konsorsium Rumah Sakit Islam Jateng-DIY.

Siswati. (2017). *Etika dan Hukum Kesehatan dalam Perspektif Undang-Undang*. Jakarta: Rajawali Pers.

Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis.c

BAB 2
KONSEP DASAR DATA KESEHATAN DAN REKAM MEDIS

Indah Naryanti, SKM, MKM

2.1 Pengertian dan Definisi Data Kesehatan

2.1.1 Definisi Data Kesehatan

Data kesehatan merupakan informasi yang mencerminkan status, kondisi, dan riwayat kesehatan individu atau populasi yang dikumpulkan, dikelola, dan dianalisis dalam konteks layanan kesehatan. Data kesehatan mencakup berbagai aspek mulai dari demografi pasien, riwayat medis, hasil pemeriksaan laboratorium, catatan diagnosis, hingga informasi pengobatan (Shen et al., 2024). Dalam era digital modern, data kesehatan telah berkembang dari sistem berbasis kertas manual menjadi sistem terintegrasi yang memanfaatkan teknologi informasi canggih untuk meningkatkan kualitas dan efisiensi layanan kesehatan.

Pentingnya data kesehatan dalam sistem kesehatan tidak dapat disangkal. Data yang berkualitas tinggi memungkinkan profesional kesehatan untuk membuat keputusan klinis yang lebih baik, mengidentifikasi tren penyakit dalam populasi, dan mengoptimalkan alokasi sumber daya kesehatan. Seiring dengan

meningkatnya kompleksitas sistem kesehatan dan pertumbuhan data medis, kebutuhan untuk menstandarisasi, mengorganisir, dan memanfaatkan data kesehatan menjadi semakin kritis (Palojoki et al., 2024). Implementasi sistem data kesehatan yang efektif memerlukan pemahaman mendalam tentang konsep, prinsip, dan teknologi yang mendasarinya.

2.1.2 Karakteristik Data Kesehatan

Data kesehatan memiliki karakteristik unik yang membedakannya dari data jenis lain. Pertama, data kesehatan sangat sensitif dan pribadi karena berisi informasi tentang kondisi fisik dan mental individu. Kedua, data kesehatan bersifat kompleks dan heterogen, mencakup data terstruktur seperti diagnosis dan hasil laboratorium, serta data tidak terstruktur seperti catatan klinis berbentuk teks bebas (Seinen et al., 2024). Karakteristik ketiga adalah bahwa data kesehatan sering kali tersebar di berbagai sistem dan lokasi, menciptakan tantangan dalam integrasi dan pertukaran informasi.

Karakteristik lain yang penting adalah bahwa data kesehatan memiliki nilai temporal yang signifikan. Informasi riwayat kesehatan pasien sepanjang waktu sangat penting untuk diagnosis dan perawatan yang akurat (Ren et al., 2024). Data kesehatan juga memiliki aspek multi-dimensi yang mencerminkan status kesehatan pasien dari perspektif berbeda, mulai dari aspek klinis, administratif, hingga finansial.

2.1.3 Jenis-jenis Data Kesehatan

Data kesehatan dapat diklasifikasikan berdasarkan berbagai dimensi. Berdasarkan strukturnya, data kesehatan dibagi menjadi data terstruktur dan data tidak terstruktur. Data terstruktur mengikuti format yang telah ditentukan sebelumnya, seperti data demografis pasien, hasil tes laboratorium yang dikode, dan diagnosis yang menggunakan sistem klasifikasi standar (Seinen et al., 2024). Data tidak terstruktur, sebaliknya, mencakup catatan klinis berbentuk narasi, laporan radiologi, dan notulen kunjungan pasien yang ditulis dalam bentuk teks bebas.

Berdasarkan jenisnya, data kesehatan mencakup data klinis yang langsung terkait dengan diagnosis dan pengobatan pasien, data administratif yang mengelola aspek operasional dan finansial, serta data demografis yang mengidentifikasi karakteristik dasar pasien. Data kesehatan juga dapat diklasifikasikan sebagai data primer atau data sekunder tergantung pada tujuan pengumpulannya, apakah untuk perawatan pasien langsung atau untuk penelitian dan analisis lebih lanjut (Alomar et al., 2024).

2.1.4 Standar dan Regulasi Data Kesehatan

Pengaturan data kesehatan memerlukan kepatuhan terhadap berbagai standar internasional dan regulasi lokal yang dirancang untuk melindungi privasi pasien dan memastikan kualitas data. Standar internasional seperti *Health Level Seven* (*HL7*), *Fast Healthcare Interoperability Resources* (*FHIR*), dan *SNOMED CT* menyediakan kerangka kerja untuk pengorganisasian,

pertukaran, dan interpretasi data kesehatan di berbagai sistem dan lembaga kesehatan (Palojoki et al., 2024). Regulasi seperti *General Data Protection Regulation* (*GDPR*) di Eropa dan *Health Insurance Portability and Accountability Act* (*HIPAA*) di Amerika Serikat menetapkan persyaratan ketat untuk perlindungan data kesehatan pribadi.

Di tingkat nasional, berbagai negara telah mengembangkan regulasi spesifik untuk pengaturan data kesehatan. Implementasi standar dan regulasi ini sangat penting tidak hanya untuk kepatuhan hukum, tetapi juga untuk membangun kepercayaan pasien terhadap sistem kesehatan digital (Riskin et al., 2025). Organisasi kesehatan harus memastikan bahwa praktik pengelolaan data mereka sesuai dengan standar internasional sambil tetap mempertimbangkan konteks dan kebutuhan lokal.

2.2 Rekam Medis Elektronik: Definisi dan Komponen

2.2.1 Pengertian Rekam Medis Elektronik

Electronic Health Record (*EHR*) atau rekam medis elektronik adalah representasi digital lengkap dari riwayat kesehatan pasien yang disimpan dan dapat diakses melalui sistem informasi komputer (Shen et al., 2024). Berbeda dengan rekam medis tradisional berbasis kertas, EHR menyediakan akses real-time ke informasi kesehatan pasien yang komprehensif dari berbagai titik layanan kesehatan. EHR bukan hanya sekadar digitalisasi catatan kertas, tetapi merupakan sistem terintegrasi yang memungkinkan

pengumpulan, penyimpanan, pengambilan, dan analisis data kesehatan dengan cara yang lebih efisien dan efektif.

Sistem *Electronic Medical Records* (*EMR*) sering kali digunakan secara bergantian dengan istilah EHR, meskipun secara teknis keduanya memiliki perbedaan. EMR biasanya mengacu pada catatan medis pasien di tingkat klinik atau rumah sakit individu, sementara EHR memiliki cakupan yang lebih luas dan dapat diakses di berbagai penyedia layanan kesehatan (Marlina et al., 2024). Adopsi EHR telah menjadi prioritas strategis dalam transformasi digital sistem kesehatan di berbagai negara, dengan tujuan meningkatkan kualitas perawatan, mengurangi kesalahan medis, dan mengoptimalkan efisiensi operasional.

2.2.2 Komponen Struktur Rekam Medis Elektronik

Rekam medis elektronik terdiri dari beberapa komponen struktural yang bekerja bersama untuk menyediakan representasi komprehensif dari status kesehatan pasien. Komponen pertama adalah data demografis pasien yang mencakup identitas, alamat, nomor kontak, dan informasi pribadi lainnya. Komponen kedua adalah data klinis yang mencakup riwayat penyakit, gejala, diagnosis, rencana pengobatan, dan hasil pengobatan (Seinen et al., 2024). Komponen ketiga adalah data laboratorium dan diagnostik yang mencakup hasil tes darah, hasil pemeriksaan pencitraan, dan data diagnostik lainnya.

Komponen-komponen lain yang penting termasuk data obat-obatan dan resep, data alergi dan kontraindikasi, data operasi dan

prosedur, serta data rujukan dan konsultasi dengan spesialis. Dalam sistem EHR modern, komponen-komponen ini terintegrasi sedemikian rupa sehingga memungkinkan akses yang mudah dan efisien ke informasi pasien yang relevan dalam konteks klinis yang spesifik (Palojoki et al., 2024). Organisasi dan struktur data dalam EHR dirancang mengikuti standar industri untuk memastikan konsistensi, interoperabilitas, dan kualitas data di berbagai sistem.

2.2.3 Fitur dan Fungsi Utama Rekam Medis Elektronik

Sistem EHR modern menawarkan berbagai fitur dan fungsi yang dirancang untuk meningkatkan efisiensi dan kualitas layanan kesehatan. Salah satu fitur utama adalah *clinical decision support system* (*CDSS*), yang memberikan rekomendasi berbasis bukti kepada profesional kesehatan saat mereka membuat keputusan klinis (Shang et al., 2024). Fitur lain termasuk sistem peringatan otomatis untuk interaksi obat yang berbahaya, kontradiksi alergi, dan hasil laboratorium yang abnormal.

Fungsi penting lainnya adalah kemampuan untuk mengintegrasikan data dari berbagai sumber dalam satu catatan pasien terpadu, memungkinkan pandangan holistik tentang status kesehatan pasien (Alomar et al., 2024). Sistem EHR juga dilengkapi dengan fitur pelaporan yang memungkinkan profesional kesehatan untuk membuat laporan klinis yang terperinci, serta fitur analitik yang mendukung penelitian klinis dan epidemiologi. Manajemen obat, penjadwalan janji temu, dan pengisian formulir digital

merupakan fungsi administratif yang juga terintegrasi dalam sistem EHR komprehensif (Razmak & Farhan, 2024).

2.2.4 Manfaat dan Tantangan Implementasi Rekam Medis Elektronik

Manfaat implementasi EHR untuk sistem kesehatan sangat beragam dan terbukti secara klinis. Peningkatan kualitas perawatan pasien melalui akses informasi yang lebih baik dan pengurangan kesalahan medis merupakan manfaat utama (Chimbo & Motsi, 2024). EHR juga memungkinkan peningkatan efisiensi operasional melalui otomasi proses administratif, pengurangan waktu tunggu, dan optimalisasi alokasi sumber daya. Dari perspektif penelitian, EHR menyediakan akses ke data pasien yang kaya untuk penelitian klinis dan epidemiologi, yang secara signifikan mempercepat pengembangan pengetahuan medis (Shen et al., 2024).

Namun, implementasi EHR juga menghadapi berbagai tantangan yang signifikan. Tantangan teknis termasuk masalah interoperabilitas antara berbagai sistem EHR yang berbeda, keamanan data, dan kualitas data yang tidak konsisten (Ren et al., 2024). Tantangan organisasi mencakup resistansi dari tenaga kesehatan terhadap perubahan, kurangnya pelatihan yang memadai, dan biaya implementasi yang tinggi. Tantangan regulasi meliputi kepatuhan terhadap berbagai standar privasi dan keamanan data yang berbeda di berbagai yurisdiksi. Mengatasi tantangan-tantangan ini memerlukan pendekatan holistik yang melibatkan investasi

teknologi, pelatihan, dan perubahan budaya organisasi (Bekele et al., 2024).

2.3 Interoperabilitas dan Pertukaran Data Kesehatan

2.3.1 Konsep Interoperabilitas dalam Sistem Kesehatan

Interoperabilitas adalah kemampuan sistem informasi kesehatan yang berbeda untuk berkomunikasi, bertukar data, dan menggunakan informasi yang diterima dengan cara yang bermakna dan efektif (Palojoki et al., 2024). Interoperabilitas merupakan elemen kritis dalam transformasi digital kesehatan karena memungkinkan pasien untuk menerima perawatan terkoordinasi dari berbagai penyedia kesehatan tanpa kehilangan informasi penting di antara sistem yang berbeda. Tingkatan interoperabilitas bervariasi dari interoperabilitas teknis (kemampuan sistem untuk bertukar data pada level teknis) hingga interoperabilitas semantik (kemampuan untuk menginterpretasi data yang ditukarkan dengan cara yang konsisten dan bermakna) (Palojoki et al., 2024).

Tantangan utama dalam mencapai interoperabilitas adalah heterogenitas sistem kesehatan yang ada. Berbagai penyedia kesehatan menggunakan sistem informasi yang berbeda, dikembangkan oleh vendor yang berbeda, dan sering kali menggunakan standar data yang berbeda-beda (Le et al., 2024). Tanpa interoperabilitas yang efektif, data pasien tetap tersebar di berbagai sistem terisolasi, menciptakan silos informasi yang menghalangi koordinasi perawatan dan menyia-nyiakan potensi dari

data kesehatan untuk penelitian dan analisis populasi (Le et al., 2024).

2.3.2 Standar Interoperabilitas dan Format Pertukaran Data

Berbagai standar internasional telah dikembangkan untuk memfasilitasi interoperabilitas dan pertukaran data kesehatan yang seragam. *Health Level Seven* (*HL7*) adalah standar paling luas yang diakui untuk pertukaran informasi klinis dan administratif dalam sistem kesehatan. *FHIR* (*Fast Healthcare Interoperability Resources*) adalah evolusi terbaru dari HL7 yang dirancang untuk memberikan pendekatan yang lebih modular, fleksibel, dan mudah diimplementasikan dalam era digital dan *web-based* (Le et al., 2024).

Selain standar pesan, terdapat pula standar untuk terminologi dan pengkodean medis seperti *SNOMED CT* (*Systematized Nomenclature of Medicine Clinical Terms*), *ICD-10* (*International Classification of Diseases*), dan *LOINC* (*Logical Observation Identifiers Names and Codes*) (Palojoki et al., 2024). Standar-standar ini memastikan bahwa konsep klinis direpresentasikan secara konsisten di berbagai sistem, memungkinkan pertukaran data yang bermakna. Implementasi standar-standar ini memerlukan komitmen organisasi yang kuat dan investasi dalam infrastruktur teknologi, tetapi manfaatnya dalam hal peningkatan kualitas data dan kemudahan pertukaran informasi sangat signifikan (Le et al., 2024).

2.3.3 Protokol dan Mekanisme Pertukaran Data

Pertukaran data kesehatan dapat dilakukan melalui berbagai mekanisme teknis yang berbeda. Pertukaran data dapat bersifat sinkron (real-time) atau asinkron (batch processing), tergantung pada kebutuhan klinis dan teknis. Implementasi berbasis *web service* seperti REST API dan *SOAP* telah menjadi standar industri untuk pertukaran data yang aman dan efisien dalam lingkungan internet modern (Le et al., 2024).

Keamanan dalam pertukaran data adalah prioritas utama, mengingat sensitivitas data kesehatan pribadi. Teknologi enkripsi end-to-end, autentikasi multi-faktor, dan protokol keamanan seperti *Transport Layer Security* (*TLS*) digunakan untuk melindungi data selama transmisi (Alhomidan et al., 2025). Selain itu, teknologi *Blockchain* semakin dipertimbangkan untuk menciptakan sistem pertukaran data yang lebih aman, transparan, dan dapat diaudit, memastikan integritas data dan menciptakan kepercayaan dalam ekosistem kesehatan digital (P et al., 2025).

2.3.4 Tantangan dan Solusi Interoperabilitas

Meskipun berbagai standar dan protokol telah dikembangkan, pencapaian interoperabilitas penuh dalam sistem kesehatan masih menghadapi banyak tantangan. Tantangan teknis termasuk implementasi standar yang tidak konsisten di berbagai vendor, kehadiran data *legacy* dalam format proprietary yang sulit untuk diintegrasikan, dan kompleksitas infrastruktur yang

ada (Palojoki et al., 2024). Tantangan non-teknis mencakup hambatan organisasi, regulasi, dan finansial.

Solusi untuk mengatasi tantangan interoperabilitas memerlukan pendekatan multi-level. Di tingkat nasional, diperlukan kepemimpinan yang kuat dan kebijakan yang jelas untuk mendorong adopsi standar (Quintero et al., 2024). Di tingkat organisasi, diperlukan investasi dalam infrastruktur teknologi, pelatihan staf, dan perubahan proses bisnis (Londoo-Puentes, 2024). Kemitraan antara penyedia kesehatan, vendor teknologi, pembuat kebijakan, dan organisasi standar internasional sangat penting untuk menciptakan ekosistem kesehatan digital yang interoperable dan efisien.

2.4 Kualitas dan Manajemen Data Kesehatan

2.4.1 Dimensi Kualitas Data Kesehatan

Kualitas data kesehatan adalah konsep multi-dimensional yang mencakup akurasi, kelengkapan, konsistensi, ketepatan waktu, dan relevansi (Riskin et al., 2025). Akurasi mengacu pada tingkat sejauh mana data kesehatan mencerminkan kondisi klinis yang sebenarnya dari pasien. Kelengkapan adalah proporsi data yang tersedia dibandingkan dengan jumlah total data yang diharapkan untuk dokumen klinis tertentu (Ren et al., 2024). Konsistensi mengacu pada keselarasan representasi data yang sama di berbagai lokasi atau sistem dalam organisasi kesehatan.

Ketepatan waktu merujuk pada ketersediaan data kesehatan pada waktu yang tepat untuk mendukung keputusan klinis dan operasional. Data yang tepat waktu sangat penting dalam konteks klinis akut di mana keputusan harus dibuat dengan cepat (Ren et al., 2024). Relevansi adalah tingkat sejauh mana data kesehatan mendukung tujuan penggunaan yang ditentukan, baik untuk perawatan pasien langsung maupun untuk penelitian dan analisis populasi.

2.4.2 Penilaian dan Pengukuran Kualitas Data

Penilaian kualitas data kesehatan memerlukan metodologi yang terstruktur dan sistematis. Pendekatan umum mencakup audit retrospektif dari catatan klinis yang ada, perbandingan data antara sumber yang berbeda, dan analisis statistik pola data untuk mengidentifikasi anomali (Riskin et al., 2025). Metrik spesifik dapat dikembangkan untuk mengukur dimensi kualitas yang berbeda. Misalnya, akurasi dapat diukur melalui validasi data terhadap standar referensi, sementara kelengkapan dapat diukur melalui perhitungan persentase field data yang terisi (Ren et al., 2024).

Penggunaan teknologi seperti *machine learning* dan *artificial intelligence* dapat meningkatkan kemampuan untuk mendeteksi dan mengkoreksi masalah kualitas data secara otomatis (Ren et al., 2024). Sistem monitoring kualitas data real-time dapat memberikan umpan balik langsung kepada pengguna tentang masalah kualitas data, memungkinkan koreksi yang lebih

cepat dan pencegahan masalah di masa depan (Kaftanov et al., 2024).

2.4.3 Strategi Peningkatan Kualitas Data

Peningkatan kualitas data kesehatan memerlukan strategi komprehensif yang melibatkan aspek teknis, organisasi, dan manusia. Langkah pertama adalah menetapkan standar kualitas data yang jelas dan terukur untuk organisasi kesehatan (Kaftanov et al., 2024). Standar-standar ini harus mencerminkan kebutuhan klinis dan operasional spesifik dari organisasi, sambil selaras dengan standar industri yang lebih luas.

Pelatihan dan pendidikan pengguna tentang pentingnya kualitas data dan praktik terbaik dalam pengumpulan dan pengelolaan data sangat penting (Marlina et al., 2024). Sistem EHR harus dirancang dengan antarmuka yang user-friendly yang mendorong pengumpulan data yang akurat dan lengkap. Fitur-fitur seperti validasi data otomatis, peringatan untuk data yang hilang atau tidak masuk akal, dan template untuk pengumpulan data yang konsisten dapat secara signifikan meningkatkan kualitas data (Ren et al., 2024). Monitoring dan audit kualitas data yang berkelanjutan diperlukan untuk mengidentifikasi tren masalah dan mengimplementasikan perbaikan yang diperlukan (Kaftanov et al., 2024).

2.4.4 Keamanan dan Privasi Data Kesehatan

Keamanan dan privasi adalah aspek kritis dari manajemen data kesehatan yang tidak dapat dikompromikan. Data kesehatan

pribadi adalah aset yang sangat berharga dan sensitif yang memerlukan perlindungan ketat terhadap akses tidak sah, penggunaan yang tidak tepat, dan pelanggaran data (Alhomidan et al., 2025). Keamanan data kesehatan memerlukan pendekatan multi-layer yang mencakup kontrol fisik, teknis, dan administratif.

Enkripsi data baik saat disimpan (at rest) maupun saat dalam transit (in transit) adalah praktek standar untuk melindungi data kesehatan (Alhomidan et al., 2025). Sistem kontrol akses berbasis peran (*role-based access control*) memastikan bahwa hanya personel yang berwenang dapat mengakses data kesehatan spesifik yang diperlukan untuk tugas mereka (P et al., 2025). Audit trail yang komprehensif yang mencatat siapa yang mengakses data apa dan kapan adalah penting untuk kepatuhan regulasi dan deteksi aktivitas mencurigakan (Alhomidan et al., 2025).

Privasi data kesehatan juga memerlukan kepatuhan terhadap regulasi seperti GDPR dan HIPAA yang menetapkan persyaratan ketat untuk persetujuan pasien, hak akses, dan penanganan permintaan penghapusan data (Alhomidan et al., 2025). Anonimisasi dan de-identifikasi data adalah teknik yang digunakan untuk melindungi privasi pasien ketika data digunakan untuk penelitian atau analisis yang tidak memerlukan identifikasi individu (Riskin et al., 2025).

2.5 Aplikasi dan Analisis Data Kesehatan

2.5.1 Penggunaan Data Kesehatan untuk Pengambilan Keputusan Klinis

Data kesehatan yang berkualitas tinggi dan terintegrasi memungkinkan pengambilan keputusan klinis yang lebih baik dan lebih berbasis bukti. Sistem *clinical decision support system* (*CDSS*) menggunakan data kesehatan historis dan real-time untuk memberikan rekomendasi kepada profesional kesehatan (Shang et al., 2024). Misalnya, algoritma pembelajaran mesin dapat menganalisis data pasien untuk memprediksi risiko penyakit tertentu, memungkinkan intervensi preventif yang lebih dini dan lebih efektif.

Integrasi data dari berbagai sumber memungkinkan profil pasien yang lebih komprehensif, yang penting untuk diagnosis akurat dan perencanaan pengobatan yang dipersonalisasi (Liu et al., 2024). Model prediktif berbasis data kesehatan dapat membantu mengidentifikasi pasien dengan risiko tinggi untuk komplikasi tertentu, memungkinkan alokasi sumber daya kesehatan yang lebih efisien (Denny, 2019).

2.5.2 Analitik Data untuk Penelitian dan Epidemiologi

Data kesehatan yang terkumpul dalam sistem EHR yang besar membuka peluang besar untuk penelitian klinis dan epidemiologi. Data dari ribuan atau jutaan pasien dapat dianalisis untuk mengidentifikasi pola penyakit, faktor risiko, dan efektivitas intervensi pada skala populasi yang sebelumnya tidak mungkin

dilakukan (Shen et al., 2024). Penelitian observasional menggunakan data kesehatan dunia nyata (*real-world data*) semakin banyak digunakan oleh regulator untuk pengambilan keputusan tentang persetujuan obat dan perangkat medis (Riskin et al., 2025).

Teknologi analitik canggih seperti *machine learning* dan *artificial intelligence* memungkinkan ekstraksi wawasan dari data kesehatan yang kompleks dan heterogen (Ren et al., 2024). Analisis dapat mengungkapkan hubungan yang tidak jelas antara faktor-faktor klinis, membantu mengidentifikasi subtipe penyakit baru, dan mengoptimalkan strategi pengobatan berdasarkan karakteristik pasien individual (Liu et al., 2024).

2.5.3 Aplikasi Data Kesehatan dalam Kesehatan Populasi

Data kesehatan juga memainkan peran penting dalam manajemen kesehatan populasi dan pencegahan penyakit pada tingkat komunitas. Sistem surveilans yang mengintegrasikan data kesehatan dari berbagai sumber dapat mendeteksi wabah penyakit dengan lebih cepat dan lebih akurat (Adirika et al., 2024). Analisis data kesehatan populasi dapat mengidentifikasi disparitas kesehatan, membantu mengalokasikan sumber daya kesehatan publik secara lebih efektif untuk mengatasi ketidaksetaraan kesehatan.

Monitoring kesehatan populasi berkelanjutan menggunakan data kesehatan real-time memungkinkan respons yang lebih cepat terhadap ancaman kesehatan yang muncul. Selama pandemi COVID-19, misalnya, data kesehatan digital memainkan peran

penting dalam pelacakan kontak, monitoring pasien, dan pengambilan keputusan kesehatan publik (Adirika et al., 2024).

2.5.4 Pelaporan dan Dashboard Kesehatan

Sistem pelaporan dan dashboard berbasis data kesehatan menyediakan visualisasi yang mudah dipahami dari metrik kesehatan penting kepada stakeholder yang berbeda (Riskin et al., 2025). Dashboard klinis memberikan informasi real-time tentang status pasien dan hasil perawatan, membantu tim klinis membuat keputusan yang lebih cepat dan lebih baik. Dashboard manajemen rumah sakit memberikan wawasan tentang operasi rumah sakit, utilisasi sumber daya, dan kinerja keuangan.

Dashboard kesehatan populasi memberikan gambaran tentang status kesehatan komunitas, membantu pembuat kebijakan dalam perencanaan kesehatan strategis dan alokasi anggaran. Visualisasi data yang efektif sangat penting untuk membuat wawasan dari data kesehatan yang kompleks dapat dipahami oleh para pengambil keputusan (Riskin et al., 2025).

Latihan Soal

1. Jelaskan perbedaan antara Electronic Medical Records (EMR) dan Electronic Health Records (EHR) serta mengapa perbedaan ini penting dalam konteks sistem kesehatan modern.
2. Diskusikan lima dimensi utama kualitas data kesehatan dan jelaskan mengapa masing-masing dimensi penting bagi keputusan klinis yang efektif.
3. Analisis tantangan utama dalam mencapai interoperabilitas data kesehatan antar sistem dan jelaskan bagaimana standar seperti FHIR dapat membantu mengatasi tantangan-tantangan ini.
4. Jelaskan bagaimana teknologi *machine learning* dan artificial intelligence dapat digunakan untuk meningkatkan kualitas data kesehatan dan apa implikasi etis yang perlu dipertimbangkan.
5. Diskusikan peran data kesehatan dalam transformasi digital sistem kesehatan dan identifikasi hambatan utama yang harus diatasi untuk realisasi potensi penuh dari data kesehatan.

DAFTAR PUSTAKA

Alomar, D., Almashmoum, M., Eleftheriou, I., Whelan, P., & Ainsworth, J. (2024). The impact of patient access to electronic health records on health care engagement: Systematic review. *JMIR Health and Uhealth*, 12, e56473. **https://doi.org/10.2196/56473**

Bawaly, M. K., Lin, C. C., Liu, C. L., & Chen, K. T. (2018). Synthesizing electronic health records using improved generative adversarial networks. *Journal of the American Medical Informatics Association*, 25(12), 1617–1624. **https://doi.org/10.1093/jamia/ocy142**

Bekele, T., Gezie, L., Willems, H., Metzger, J., Abere, B., Seyoum, B., Abraham, L., Wendrad, N., Meressa, S., Desta, B., & Bogale, T. (2024). Barriers and facilitators of the electronic medical record adoption among healthcare providers in Addis Ababa, Ethiopia. *SAGE Open Nursing*, 10, 23779608241301946. **https://doi.org/10.1177/23779608241301946**

Chatgpt, A., Pahari, N., & Prinz, A. (2022). HL7 FHIR with SNOMED-CT to achieve semantic and structural interoperability in personal health data: A proof-of-concept study. *Sensors*, 22(10), 3756. **https://doi.org/10.3390/s22103756**

Chimbo, B., & Motsi, L. (2024). The effects of electronic health records on medical error reduction: Extension of the DeLone

and McLean information system success model. *JMIR Medical Education*, 10, e54572. **https://doi.org/10.2196/54572**

Denny, J. C. (2019). The All of Us Research Program. *New England Journal of Medicine*, 381(7), 668–676. **https://doi.org/10.1056/NEJMsr1809937**

Kruse, C. S., Stein, A., Thomas, H., & Kaur, H. (2018). The use of electronic health records to support population health: A systematic review of the literature. *Journal of Medical Systems*, 42(11), 214. **https://doi.org/10.1007/s10916-018-1075-6**

Palojoki, S., Lehtonen, L., & Vuokko, R. (2024). Semantic interoperability of electronic health records: Systematic review of alternative approaches for enhancing patient information availability. *JMIR Medical Informatics*, 12, e53535. **https://doi.org/10.2196/53535**

Rajkomar, A., Oren, E., Chen, K., Dai, A. M., Hajaj, N., Hardt, M., Liu, P. J., Liu, X., Marcus, J., Sun, M., Sundberg, P., Yee, H., Zhang, K., Zhang, Y., Flores, G., Duggan, G. E., Irvine, J., Le, Q. V., Litsch, K., ... Dean, J. (2018). Scalable and accurate deep learning with electronic health records. *NPJ Digital Medicine*, 1, 18. **https://doi.org/10.1038/s41746-018-0029-1**

Ren, W., Liu, Z., Wu, Y., Zhang, Z., Hong, S., & Liu, H. (2024). Moving beyond medical statistics: A systematic review on

missing data handling in electronic health records. *Health Data Science*, 4, e0176. **https://doi.org/10.34133/hds.0176**

Shen, Y., Yu, J., Zhou, J., & Hu, G. (2024). Twenty-five years of evolution and hurdles in electronic health records and interoperability in medical research: Comprehensive review. *JMIR Medical Informatics*, 12, e59024. **https://doi.org/10.2196/59024**

BAB 3
PRINSIP KEAMANAN DATA & INFORMASI

Arief Azhari Ilyas, A.Md.RMIK., S.St., M.K.M

3.1 Fondasi Prinsip Keamanan Data

3.1.1 Definisi dan Konsep Keamanan Data

Keamanan data merupakan praktik fundamental dalam melindungi informasi sensitif dari akses tidak sah, modifikasi, atau penghancuran melalui serangkaian mekanisme teknis dan organisasi yang terkoordinasi dengan baik. Keamanan data tidak hanya mencakup perlindungan fisik informasi, tetapi juga melibatkan perlindungan logis terhadap ancaman siber yang terus berkembang di era digital (Paiman et al., 2025). Konsep keamanan data berpusat pada tiga pilar fundamental yang dikenal sebagai *CIA Triad*: *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan). Ketiga pilar ini membentuk dasar pemahaman tentang bagaimana data harus dikelola, dilindungi, dan diakses oleh organisasi modern.

Kerahasiaan berarti bahwa data sensitif hanya dapat diakses oleh individu atau sistem yang berwenang, sementara integritas memastikan bahwa data tetap akurat, konsisten, dan tidak diubah tanpa izin. Ketersediaan, di sisi lain, menjamin bahwa data dan

sistem dapat diakses kapan pun diperlukan oleh pengguna yang sah (Narne & Dholakia, 2025).

Dalam konteks pelayanan kesehatan di Indonesia, prinsip-prinsip keamanan data telah diadopsi secara eksplisit dan diamanatkan dalam Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. Regulasi ini menegaskan bahwa Rekam Medis Elektronik wajib memenuhi prinsip keamanan data dan informasi yang meliputi kerahasiaan (*confidentiality*), yaitu jaminan keamanan data dari gangguan pihak tidak berhak; integritas (*integrity*), yakni jaminan terhadap keakuratan data yang perubahannya hanya dapat dilakukan oleh pihak yang memiliki otorisasi; serta ketersediaan (*availability*), yaitu jaminan bahwa data dapat diakses oleh pengguna yang telah mendapatkan hak akses dari pimpinan fasilitas pelayanan kesehatan.

Dengan demikian, ketiga pilar CIA Triad telah menjadi standar hukum yang wajib dipenuhi dalam penyelenggaraan rekam medis elektronik, sejalan dengan transformasi digital layanan kesehatan yang mengedepankan keamanan dan kerahasiaan data. Untuk menjamin implementasinya, peraturan ini mengatur pemberian hak akses bertingkat kepada tenaga kesehatan meliputi hak input, perbaikan, dan akses data yang merupakan penerapan nyata dari prinsip *least privilege*, di mana setiap individu hanya mendapatkan akses sesuai kewenangan dan kebutuhannya.

Dalam konteks modern, terutama dengan meningkatnya ketergantungan pada *cloud computing*, kecerdasan buatan, dan

Internet of Things (*IoT*), keamanan data telah menjadi isu strategis yang memengaruhi reputasi organisasi, kepercayaan pelanggan, dan kepatuhan terhadap regulasi internasional (Kandregula, 2025).

3.1.2 Ancaman dan Risiko Keamanan Data

Lanskap ancaman keamanan siber terus berkembang dengan kompleksitas dan tingkat kecanggihan yang meningkat. Ancaman umum terhadap keamanan data mencakup *malware*, *ransomware*, serangan *phishing*, *denial of service* (*DDoS*), dan *social engineering*. Serangan ini memanfaatkan kerentanan dalam sistem teknologi informasi maupun faktor manusia seperti kurangnya kesadaran keamanan karyawan. *Ransomware*, khususnya, telah menjadi ancaman yang sangat serius karena kemampuannya mengenkripsi data kritis dan meminta pembayaran untuk pemulihan, menyebabkan kerugian finansial yang signifikan bagi organisasi (Agunuru, 2025).

Risiko keamanan data bukan hanya berasal dari ancaman eksternal, tetapi juga dari insider threats atau ancaman dari dalam organisasi, termasuk karyawan yang tidak puas atau yang mencoba mengakses data di luar wewenang mereka. Dengan meningkatnya penggunaan perangkat mobile dan *cloud computing*, permukaan serangan telah berkembang secara eksponensial, menciptakan tantangan baru dalam manajemen keamanan data. Organisasi harus mengidentifikasi aset informasi mereka yang paling berharga, mengevaluasi kemungkinan dan dampak potensial dari berbagai

ancaman, serta mengembangkan strategi mitigasi yang proporsional dengan risiko yang dihadapi.

3.1.3 Kerangka Kerja Keamanan Data Internasional

Beberapa kerangka kerja internasional telah ditetapkan untuk memandu organisasi dalam mengimplementasikan praktik keamanan data yang robust. ISO/IEC 27001 adalah standar internasional yang paling banyak diadopsi, menyediakan persyaratan komprehensif untuk sistem manajemen keamanan informasi (*Information Security Management System* atau ISMS) (Hosan, 2025). *NIST Cybersecurity Framework*, yang dikembangkan oleh *National Institute of Standards and Technology*, menawarkan pendekatan fleksibel yang dapat disesuaikan dengan konteks organisasi spesifik dan mencakup lima fungsi inti: *Identify*, *Protect*, *Detect*, *Respond*, dan *Recover* (Rahman et al., 2024).

Kerangka kerja ini memberikan panduan praktis tentang bagaimana organisasi dapat mengevaluasi postur keamanan mereka, mengidentifikasi area untuk perbaikan, dan menerapkan kontrol keamanan yang efektif. Selain itu, *Center for Internet Security* (*CIS*) menawarkan seperangkat kontrol keamanan yang prioritasnya didasarkan pada riset dan pengalaman praktik industri. Organisasi yang berbeda mungkin memilih kerangka kerja yang berbeda berdasarkan industri mereka, ukuran organisasi, dan persyaratan regulasi spesifik yang mereka hadapi (Ajisegiri et al., 2025).

3.1.4 Paradigma Keamanan Modern

Paradigma keamanan data telah berkembang dari pendekatan *perimeter-based security* tradisional menuju pendekatan *zero-trust* yang lebih holistik (Wang et al., 2025). Model keamanan berbasis perimeter mengasumsikan bahwa segala sesuatu di dalam jaringan organisasi dapat dipercaya, sementara segala sesuatu di luar dianggap tidak dapat dipercaya. Pendekatan ini tidak lagi memadai dalam era di mana karyawan bekerja dari mana saja, mengakses berbagai *cloud services*, dan perangkat yang beragam terhubung ke jaringan.

Paradigma *zero-trust* menerapkan prinsip "tidak pernah mempercayai, selalu memverifikasi" (*never trust, always verify*), yang berarti setiap akses ke data dan sistem harus diverifikasi, terlepas dari apakah akses tersebut berasal dari dalam atau luar jaringan organisasi (Saidyetal., 2024). Pendekatan ini mengintegrasikan *multi-factor authentication*, enkripsi *end-to-end*, monitoring berkelanjutan, dan analitik perilaku pengguna untuk mendeteksi anomali dan ancaman potensial. Selain itu, organisasi semakin mengadopsi pendekatan *security-by-design*, di mana pertimbangan keamanan diintegrasikan ke dalam setiap tahap pengembangan sistem informasi, bukan hanya ditambahkan kemudian sebagai fitur tambahan (Kandregula, 2025).

3.2 Regulasi dan Kepatuhan Keamanan Data

3.2.1 Peraturan Perlindungan Data Global

Regulasi perlindungan data telah menjadi landasan hukum yang mengatur bagaimana organisasi harus menangani informasi pribadi. *General Data Protection Regulation* (GDPR) dari Uni Eropa, yang berlaku sejak Mei 2018, telah menjadi standar emas untuk perlindungan data pribadi dengan persyaratan yang ketat dan cakupan global (Gilbert & Gilbert, 2025). GDPR menerapkan prinsip-prinsip seperti *data minimization* (pengumpulan data minimal), *purpose limitation* (pembatasan tujuan), dan *storage limitation* (pembatasan penyimpanan), serta memberikan hak yang signifikan kepada subjek data seperti hak untuk dihapus (*right to be forgotten*) dan hak untuk akses.

Di Amerika Serikat, regulasi berbeda antar negara bagian, dengan *California Consumer Privacy Act* (CCPA) menjadi salah satu yang paling komprehensif. Regulasi lain seperti *Health Insurance Portability and Accountability Act* (HIPAA) untuk industri kesehatan, *Payment Card Industry Data Security Standard* (PCI DSS) untuk pemrosesan data kartu kredit, dan regulasi spesifik sektor lainnya menetapkan persyaratan keamanan yang ketat (Shah, 2023). Negara-negara lain juga mengembangkan regulasi sendiri, seperti LGPD di Brasil dan Personal Data Protection Law di Indonesia, mencerminkan pengakuan global tentang pentingnya perlindungan data.

3.2.2 Kepatuhan Regulasi dan Tantangannya

Kepatuhan terhadap regulasi perlindungan data merupakan keharusan hukum dan strategis bagi organisasi, tetapi juga

menghadirkan tantangan signifikan. Organisasi yang beroperasi di berbagai yurisdiksi harus menavigasi lanskap regulasi yang kompleks dan terkadang saling bertentangan. Misalnya, persyaratan GDPR tentang perlindungan data pribadi dapat berbenturan dengan undang-undang nasional di negara lain yang mengharuskan pelokalan data atau memberikan akses kepada otoritas pemerintah.

Tantangan kepatuhan mencakup biaya implementasi yang tinggi, terutama untuk organisasi kecil dan menengah, kebutuhan akan keahlian khusus dalam memahami regulasi yang kompleks, dan beban administratif untuk mendokumentasikan dan melaporkan kepatuhan. Selain itu, regulasi terus berkembang untuk mengakomodasi teknologi baru seperti *artificial intelligence* dan *machine learning*, memerlukan organisasi untuk terus memperbarui praktik keamanan dan kebijakan mereka. Organisasi juga harus mengintegrasikan kepatuhan regulasi ke dalam budaya organisasi mereka, tidak hanya sebagai fungsi kepatuhan tetapi sebagai tanggung jawab yang dibagikan di seluruh organisasi (Pokhidnia, 2025).

3.2.3 Audit dan Penilaian Keamanan

Audit dan penilaian keamanan adalah mekanisme penting untuk memverifikasi bahwa organisasi mematuhi persyaratan regulasi dan standar keamanan yang relevan. Audit internal dilakukan oleh tim organisasi sendiri untuk mengevaluasi kepatuhan terhadap kebijakan internal dan standar industri, sementara audit eksternal dilakukan oleh pihak ketiga independen untuk memberikan

perspektif objektif (Rahman et al., 2024). Penilaian kerentanan sistem informasi mengidentifikasi titik lemah dalam infrastruktur keamanan yang dapat dieksploitasi oleh penyerang.

Penetration testing adalah teknik yang mensimulasikan serangan nyata untuk menguji efektivitas pertahanan keamanan organisasi. Organisasi juga harus melakukan *data protection impact assessments* (DPIA) untuk mengidentifikasi risiko privasi dan keamanan yang terkait dengan pemrosesan data pribadi, terutama ketika menerapkan teknologi baru atau mengubah praktik pemrosesan data mereka (Galandarli, 2025). Hasil audit dan penilaian ini harus didokumentasikan dengan baik dan digunakan untuk mengidentifikasi area perbaikan serta mengalokasikan sumber daya untuk mengatasi kerentanan keamanan.

3.2.4 Respons Insiden dan Manajemen Krisis

Organisasi harus memiliki rencana respons insiden yang komprehensif untuk menangani pelanggaran keamanan data dengan cepat dan efektif. Rencana ini harus mencakup prosedur untuk mendeteksi insiden, membatasi dampak, menginformasikan pihak yang terkena, dan melakukan investigasi untuk memahami penyebab insiden. Dalam banyak regulasi, ada persyaratan untuk melaporkan pelanggaran data kepada otoritas regulasi dan individu yang terkena dalam jangka waktu yang ditentukan.

Manajemen krisis dalam konteks keamanan data melibatkan koordinasi antara berbagai departemen organisasi, komunikasi yang jelas dengan *stakeholder* eksternal, dan pembelajaran dari insiden

untuk mencegah kejadian serupa di masa depan. Tim respons insiden harus terlatih dan siap untuk merespons dengan cepat, dan organisasi harus melakukan simulasi rutin untuk memastikan kesiapan. Transparansi dalam menangani pelanggaran data, meskipun menantang secara reputasi, dapat membantu mempertahankan kepercayaan pelanggan dan menunjukkan komitmen organisasi terhadap keamanan data.

3.3 Teknologi Keamanan Data

3.3.1 Enkripsi dan Teknik Perlindungan Data

Enkripsi adalah salah satu alat keamanan paling fundamental untuk melindungi kerahasiaan data dengan mengubah data yang dapat dibaca (*plaintext*) menjadi format yang tidak dapat dibaca (*ciphertext*) tanpa kunci dekripsi yang tepat. Enkripsi dapat diterapkan pada data saat istirahat (*at rest*) di penyimpanan, data dalam transit (*in transit*) melalui jaringan, dan bahkan pada data yang sedang diproses (*in use*) (C et al., 2023). Teknik enkripsi simetris, seperti AES (*Advanced Encryption Standard*), menggunakan kunci yang sama untuk enkripsi dan dekripsi, sementara teknik asimetris, seperti RSA, menggunakan sepasang kunci publik dan privat (Narne & Dholakia, 2025).

Selain enkripsi, organisasi dapat menggunakan teknik perlindungan data lainnya seperti *masking*, yang menyembunyikan sebagian dari data sensitif tanpa menghilangkannya sepenuhnya, dan *anonymization*, yang menghapus atau mengubah informasi

pengidentifikasi pribadi sehingga individu tidak dapat diidentifikasi. *Tokenization* adalah teknik lain di mana data sensitif diganti dengan token yang tidak memiliki nilai instrinsik kecuali dalam konteks spesifik organisasi. Organisasi juga harus mempertimbangkan penggunaan *differential privacy*, teknik yang memungkinkan analisis data sambil melindungi privasi individu dengan menambahkan noise statistik ke data atau hasil query (Yin et al., 2021).

3.3.2 Kontrol Akses dan Manajemen Identitas

Kontrol akses adalah mekanisme untuk memastikan bahwa hanya pengguna yang berwenang dapat mengakses data dan sistem tertentu. Pendekatan *role-based access control* (RBAC) memberikan izin kepada pengguna berdasarkan peran mereka dalam organisasi, sementara *attribute-based access control* (ABAC) mempertimbangkan berbagai atribut pengguna, sumber daya, dan lingkungan untuk membuat keputusan akses yang lebih granular (Hosan, 2025). *Multi-factor authentication* (MFA), yang menggabungkan dua atau lebih metode autentikasi seperti kata sandi dan kode dari aplikasi mobile, meningkatkan keamanan dengan membuat lebih sulit bagi penyerang untuk mendapatkan akses yang tidak sah (Yeswanth & Guntaka, 2026).

Penerapan kontrol akses dan manajemen identitas juga mencakup autentikasi pengguna saat mencatatkan data, misalnya melalui Tanda Tangan Elektronik (TTE). Namun, penelitian Ilyas et al. (2025) menemukan bahwa meskipun rumah sakit telah

mengimplementasikan RME dengan TTE, aspek autentikasi yang kuat masih menjadi kendala. TTE yang digunakan belum tersertifikasi oleh Penyelenggara Sertifikasi Elektronik (PSrE), sehingga legalitasnya diragukan dan berdampak pada penolakan klaim BPJS. Kasus ini menegaskan bahwa implementasi TTE harus dibarengi dengan pemenuhan aspek legal dan standar keamanan agar fungsi autentikasi dan integritas data dapat diakui secara sah oleh pihak eksternal.

Manajemen identitas dan akses (IAM) adalah disiplin yang lebih luas yang mencakup proses untuk mengelola identitas digital pengguna, memverifikasi identitas mereka, dan mengelola izin akses mereka sepanjang siklus hidup mereka dalam organisasi. Sistem IAM modern mengintegrasikan *single sign-on* (SSO), *identity federation*, dan mekanisme *provisioning* otomatis untuk meningkatkan efisiensi dan keamanan. Organisasi juga harus menerapkan prinsip *least privilege*, yang memberikan pengguna hanya izin minimum yang diperlukan untuk melakukan tugas mereka (Wang et al., 2025).

3.3.3 Pemantauan dan Deteksi Ancaman

Pemantauan keamanan berkelanjutan adalah kunci untuk mendeteksi dan merespons ancaman dengan cepat. *Security Information and Event Management* (SIEM) mengintegrasikan log dan data peristiwa dari berbagai sumber sistem informasi untuk memberikan visibilitas menyeluruh tentang lanskap keamanan organisasi. SIEM dapat mengkorelasikan peristiwa dari sumber yang

berbeda untuk mengidentifikasi pola yang mengindikasikan aktivitas berbahaya, seperti upaya login yang berulang kali atau transfer data yang tidak biasa.

User and Entity Behavior Analytics (UEBA) menggunakan analitik dan *machine learning* untuk membangun profil perilaku normal pengguna dan entitas sistem, kemudian mendeteksi anomali yang mungkin menunjukkan kompromi atau aktivitas yang tidak sah (Agunuru, 2025). Sistem deteksi ancaman berbasis AI dapat mengidentifikasi pola serangan yang belum pernah terlihat sebelumnya dengan menganalisis karakteristik perilaku dari malware dan perubahan sistem yang mencurigakan. Organisasi juga harus mengintegrasikan *threat intelligence*, yang mengumpulkan dan menganalisis informasi tentang ancaman yang dihadapi organisasi atau industri mereka, untuk menginformasikan strategi keamanan mereka (Nadella et al., 2025).

3.3.4 Pembelajaran Mesin dan Kecerdasan Buatan dalam Keamanan

Artificial Intelligence dan *machine learning* memiliki potensi besar untuk meningkatkan keamanan data melalui deteksi anomali otomatis, prediksi ancaman, dan respons ancaman yang dipercepat (Agunuru, 2025). Model pembelajaran mesin dapat dilatih pada data historis untuk mengidentifikasi pola yang terkait dengan aktivitas berbahaya, memungkinkan sistem keamanan untuk bereaksi terhadap ancaman dengan lebih cepat daripada analis keamanan manusia. *Federated learning*, pendekatan di mana model

pembelajaran mesin dilatih secara terdistribusi pada data lokal tanpa mengumpulkan semua data di lokasi pusat, menawarkan cara untuk meningkatkan keamanan sambil mempertahankan privasi data (Rahmati, 2025).

Namun, penggunaan AI dalam keamanan juga membawa risiko, seperti kemungkinan bias dalam model yang dilatih pada data historis yang tidak representatif, kerentanan terhadap serangan yang dirancang khusus untuk menipu model AI, dan kurangnya transparansi dalam bagaimana model AI membuat keputusan. Organisasi harus memilih solusi keamanan berbasis AI dengan hati-hati, memverifikasi efektivitasnya, dan terus memonitor kinerja untuk memastikan bahwa solusi tersebut tetap efektif terhadap ancaman yang berkembang (Ogunmolu, 2025).

3.4 Praktik Terbaik Keamanan Data

3.4.1 Keamanan Desain dan Privasi Sejak Awal

Privacy by design dan *security by design* adalah pendekatan proaktif untuk mengintegrasikan pertimbangan privasi dan keamanan ke dalam setiap tahap pengembangan sistem informasi, bukan hanya menambahkannya sebagai fitur setelah sistem dikembangkan (Ogbodo et al., 2025). Pendekatan ini dimulai dengan memahami persyaratan privasi dan keamanan yang dikenakan oleh regulasi dan standar industri, kemudian mengintegrasikan persyaratan tersebut ke dalam spesifikasi sistem, desain arsitektur, dan proses pengembangan.

Prinsip *security by design* menekankan pentingnya perencanaan keamanan sejak awal pengembangan sistem. Namun, penelitian Ilyas et al. (2023) menunjukkan konsekuensi dari tidak diterapkannya prinsip ini. RME yang diterapkan sejak 2019 belum mengacu pada pedoman resmi karena saat itu belum tersedia, sehingga ketika Kepmenkes No. 1423 Tahun 2022 terbit, ditemukan banyak ketidaksesuaian seperti modul *general consent*, asesmen psikologis, dan *informed consent* elektronik yang tidak terintegrasi. Akibatnya, terjadi ketidaklengkapan data serta risiko pelanggaran privasi dan legalitas, terutama karena TTE pasien juga belum tersedia. Kasus ini menegaskan bahwa kegagalan merancang sistem dengan mengacu pada standar yang relevan, meskipun regulasi mungkin belum ada saat pengembangan dapat menimbulkan masalah kepatuhan di kemudian hari. Selain itu, penelitian ini juga menyoroti tantangan sumber daya, di mana setiap perubahan variabel dalam RME memerlukan anggaran tambahan untuk vendor, sejalan dengan tantangan implementasi keamanan yang telah dibahas sebelumnya.

Secure software development lifecycle (SSDLC) mencakup praktik pengembangan yang aman pada setiap tahap, mulai dari analisis kebutuhan hingga pemeliharaan berkelanjutan (Kandregula, 2025). In i termasuk penggunaan *static application security testing* (SAST) dan *dynamic application security testing* (DAST) untuk mengidentifikasi kerentanan dalam kode, praktik *code review* yang ketat, dan pengujian keamanan yang sistematis sebelum

sistem diproduksi. Organisasi juga harus melakukan penilaian risiko keamanan reguler dan memperbarui desain mereka berdasarkan ancaman yang muncul dan pembelajaran dari insiden keamanan.

3.4.2 Kesadaran Keamanan dan Pelatihan Karyawan

Faktor manusia tetap menjadi salah satu kerentanan terbesar dalam keamanan data, dengan *phishing*, *social engineering*, dan kesalahan pengguna yang tidak disengaja menjadi penyebab utama dari banyak pelanggaran keamanan. Program kesadaran keamanan yang efektif harus mencakup pelatihan reguler untuk semua karyawan tentang praktik keamanan yang baik, pengenalan ancaman keamanan umum, dan prosedur untuk melaporkan insiden keamanan yang mencurigakan. Pelatihan harus disesuaikan dengan peran spesifik karyawan, dengan karyawan yang menangani data sensitif menerima pelatihan yang lebih mendalam.

Penelitian Golo et al. (2023) memberikan bukti empiris bahwa faktor individu meliputi persepsi kegunaan, kemudahan penggunaan, minat perilaku, dan penggunaan actual berpengaruh signifikan dan positif terhadap implementasi RME. Sebaliknya, faktor organisasional seperti dukungan manajemen puncak dan budaya organisasi justru menunjukkan pengaruh negatif yang tidak signifikan. Temuan ini menegaskan bahwa keberhasilan implementasi sistem keamanan dan teknologi baru sangat bergantung pada penerimaan dan kesiapan individu penggunanya. Resistensi individu yang tidak terkelola dapat menggagalkan adopsi teknologi, meskipun dukungan organisasi telah tersedia. Oleh karena

itu, program pelatihan dan pendampingan yang berfokus pada peningkatan literasi digital dan keyakinan individu menjadi urgen; tanpa intervensi tepat sasaran pada level individu, investasi infrastruktur dan kebijakan organisasi mungkin tidak membuahkan hasil optimal.

Organisasi juga harus menciptakan budaya keamanan di mana karyawan merasa nyaman melaporkan insiden keamanan tanpa takut akan hukuman, dan di mana keamanan dihargai sebagai tanggung jawab bersama daripada hanya tanggung jawab departemen IT. *Gamification*, penggunaan mekanisme permainan dalam program pelatihan keamanan, telah terbukti meningkatkan engagement dan retensi pengetahuan keamanan. Organisasi juga harus melakukan simulasi *phishing* reguler dan *tabletop exercises* untuk menguji kesiapan organisasi terhadap ancaman keamanan dan mengidentifikasi area untuk perbaikan.

3.4.3 Manajemen Vendor dan Rantai Pasokan

Dengan meningkatnya penggunaan vendor eksternal, *cloud service providers*, dan mitra bisnis, manajemen risiko keamanan dalam rantai pasokan telah menjadi semakin penting. Organisasi harus melakukan penilaian keamanan yang ketat terhadap vendor sebelum melibatkan mereka untuk menangani data sensitif, termasuk evaluasi kontrol keamanan mereka, sertifikasi keamanan, dan riwayat insiden keamanan. Kontrak dengan vendor harus mencakup klausul keamanan yang jelas yang menetapkan tanggung jawab vendor untuk melindungi data, persyaratan untuk melaporkan

insiden keamanan, dan hak organisasi untuk melakukan audit keamanan.

Studi yang dilakukan oleh Ilyas et al (2023) menyoroti risiko ketergantungan pada vendor dalam pengelolaan Rekam Medis Elektronik (RME), di mana setiap penyesuaian sistem terhadap regulasi baru harus melalui persetujuan vendor dan otorisasi direktur yang berdampak pada anggaran, sehingga memperlambat adaptasi organisasi terhadap perubahan regulasi. Kasus ini menegaskan kerentanan dalam rantai pasok digital, di mana minimnya kendali internal dapat menghalangi penerapan prinsip *security by design* yang adaptif. Untuk itu, organisasi disarankan memiliki tim IT internal yang kompeten atau menyusun kontrak vendor yang fleksibel guna memastikan kepatuhan dan keamanan sistem dapat ditingkatkan secara berkelanjutan tanpa kendala birokrasi yang berlebihan.

Organisasi juga harus melakukan monitoring berkelanjutan terhadap keamanan vendor melalui evaluasi berkala, review log audit, dan *vulnerability assessments*. Jika seorang vendor dikompromikan oleh penyerang, hal itu dapat memiliki dampak yang signifikan pada organisasi Anda, seperti yang ditunjukkan oleh berbagai serangan rantai pasokan besar-besaran dalam beberapa tahun terakhir. Organisasi harus memiliki rencana kontingensi untuk mengalihkan ke vendor alternatif jika vendor mereka saat ini mengalami insiden keamanan yang serius.

3.4.4 Pengembangan dan Pembaruan Kebijakan Keamanan

Kebijakan keamanan yang komprehensif dan terdokumentasi dengan baik adalah fondasi dari program keamanan data yang efektif. Kebijakan harus mencakup standar untuk perlindungan data, kontrol akses, penggunaan perangkat, penggunaan internet, dan prosedur respons insiden. Kebijakan harus ditulis dalam bahasa yang jelas dan dapat dipahami oleh semua karyawan, bukan hanya profesional IT, dan harus dikomunikasikan secara luas di seluruh organisasi.

Kebijakan keamanan harus diperbarui secara berkala untuk mencerminkan perubahan dalam lanskap ancaman, regulasi baru, dan pembelajaran dari insiden keamanan. Organisasi harus melakukan review paling tidak setahun sekali, dan mungkin lebih sering jika ada perubahan signifikan dalam operasi organisasi atau lingkungan keamanan. Semua karyawan harus menandatangani pengakuan kebijakan keamanan untuk memastikan bahwa mereka memahami tanggung jawab mereka dan konsekuensi dari pelanggaran kebijakan (Pokhidnia, 2025).

3.5 Tantangan Masa Depan dalam Keamanan Data

3.5.1 Komputasi Kuantum dan Kriptografi Pasca-Kuantum

Kemajuan dalam komputasi kuantum menghadirkan ancaman potensial terhadap algoritma enkripsi yang saat ini digunakan untuk melindungi data sensitif. Komputer kuantum, sekali tersedia dalam skala besar, akan dapat memecahkan algoritma

enkripsi berbasis faktorisasi seperti RSA dalam waktu yang relatif singkat, mengancam keamanan data yang dienkripsi dengan metode tradisional. Organisasi harus mulai bersiap untuk transisi menuju algoritma kriptografi yang tahan terhadap serangan kuantum (*post-quantum cryptography*) sebelum ancaman ini menjadi kenyataan.

Pemerintah dan badan standar internasional sudah bekerja pada pengembangan dan standarisasi algoritma kriptografi pasca-kuantum yang dapat menahan serangan dari komputer kuantum. Organisasi harus memulai inventaris enkripsi mereka saat ini, mengidentifikasi data yang sangat sensitif dengan lama waktu perlindungan jangka panjang, dan merencanakan migrasi ke algoritma kriptografi pasca-kuantum (Ogunmolu, 2025). Ini akan memerlukan investasi signifikan dalam infrastruktur keamanan dan koordinasi lintas organisasi.

3.5.2 Keamanan dalam Teknologi Emerging

Artificial Intelligence, *Internet of Things*, *Blockchain*, dan teknologi emerging lainnya membawa peluang baru tetapi juga tantangan keamanan yang signifikan. Perangkat *IoT* sering kali memiliki sumber daya yang terbatas, sehingga sulit untuk mengimplementasikan kontrol keamanan standar yang biasanya diterapkan pada komputer desktop atau server. Sistem *Blockchain*, meskipun dirancang dengan transparansi dan keamanan dalam pikiran, tetap memiliki kerentanan seperti *smart contract bugs* dan serangan pada protokol konsensus (Monrat et al., 2019).

Organisasi yang mengadopsi teknologi emerging ini harus melakukan penilaian keamanan yang teliti, bekerja sama dengan peneliti keamanan dan penyedia teknologi untuk mengidentifikasi dan mengatasi kerentanan sebelum teknologi ini diproduksi pada skala besar. Organisasi juga harus terus memantau perkembangan ancaman baru yang menargetkan teknologi ini dan memperbarui strategi keamanan mereka sesuai kebutuhan (Rahmati & Pagano, 2025).

3.5.3 Keseimbangan antara Keamanan dan Privasi

Mengimplementasikan keamanan data yang ketat dapat mengurangi aksesibilitas data bagi pengguna yang sah, menciptakan ketegangan antara keamanan dan kegunaan. Organisasi harus menemukan keseimbangan yang tepat antara implementasi kontrol keamanan yang kuat dan mempertahankan kegunaan sistem yang wajar. Ini mungkin melibatkan penggunaan teknologi yang inovatif seperti *privacy-preserving techniques* yang memungkinkan analisis data sambil melindungi privasi individu.

Selain itu, meningkatkan keamanan data sering kali memerlukan pengumpulan dan penyimpanan data tentang aktivitas pengguna untuk tujuan pemantauan dan deteksi ancaman. Organisasi harus memastikan bahwa praktik pemantauan ini tidak melampaui apa yang diperlukan dan bahwa data pemantauan itu sendiri dilindungi dengan baik terhadap akses yang tidak sah. Transparansi tentang praktik keamanan dan privasi dari organisasi

adalah penting untuk membangun kepercayaan dengan pengguna dan *stakeholder*.

3.5.4 Keberlanjutan Program Keamanan Data

Mempertahankan program keamanan data yang efektif dalam jangka panjang adalah tantangan signifikan, terutama karena lanskap ancaman terus berubah dan regulasi terus berkembang. Banyak organisasi mengalami *security fatigue*, di mana karyawan menjadi lelah dengan peringatan keamanan yang terus-menerus dan permintaan untuk mematuhi kebijakan keamanan yang ketat, yang dapat menyebabkan mereka mengabaikan atau bahkan mengakali kontrol keamanan. Organisasi harus mendesain program keamanan mereka dengan cara yang berkelanjutan, fokus pada pelatihan dan kesadaran yang berkelanjutan daripada hanya penegakan aturan, dan menciptakan budaya di mana keamanan dilihat sebagai bagian integral dari operasi bisnis daripada sesuatu yang ditambahkan dari luar.

Hal ini sejalan dengan Ilyas, et. al (2025) yang memaparkan bahwa keberlanjutan keamanan data seperti sistem rekam medis *hybrid* memerlukan pendekatan holistik mencakup aspek teknis, tata kelola, dan sumber daya manusia. Strategi pengamanan menyeluruh meliputi enkripsi, pengamanan fisik, serta kebijakan akses ketat dengan prinsip *least privilege* menjadi kunci untuk mengatasi risiko ganda kehilangan dokumen kertas dan kebocoran data digital. Selain itu, audit terstruktur yang mampu memverifikasi konsistensi antara data manual dan elektronik melalui metode seperti *double data*

entry sangat diperlukan untuk menjaga integritas data jangka panjang. Tidak kalah penting, kompetensi SDM merupakan fondasi utama keberlanjutan program keamanan, di mana organisasi harus membangun kemampuan teknis, motivasi digital, serta peluang pengembangan staf secara berkelanjutan. Dengan demikian, keamanan data yang berkelanjutan hanya dapat dicapai jika teknologi, proses audit, dan kapabilitas manusia dikelola secara terintegrasi dan berkesinambungan.

Latihan Soal

1. Jelaskan ketiga pilar dari CIA Triad (Confidentiality, Integrity, Availability) dan bagaimana masing-masing pilar berperan dalam melindungi keamanan data organisasi. Berikan contoh konkret tentang bagaimana pelanggaran terhadap setiap pilar dapat berdampak pada organisasi. Bagaimana organisasi dapat memastikan bahwa ketiga pilar ini seimbang tanpa mengorbankan kegunaan sistem?
2. Diskusikan perbedaan antara model keamanan berbasis perimeter tradisional dan paradigma Zero Trust Architecture. Apa keuntungan dan tantangan dari mengimplementasikan Zero Trust Architecture dalam organisasi yang kompleks? Apa saja komponen teknologi utama yang diperlukan untuk mendukung implementasi yang sukses?
3. Analisis dampak dari regulasi perlindungan data global seperti GDPR, CCPA, dan regulasi lokal terhadap operasi organisasi

yang beroperasi secara internasional. Apa tantangan utama yang dihadapi organisasi dalam mencapai kepatuhan terhadap regulasi yang berbeda di berbagai yurisdiksi? Bagaimana organisasi dapat mengembangkan strategi kepatuhan yang efisien dan cost-effective?

4. Jelaskan mengapa faktor manusia tetap menjadi kerentanan terbesar dalam keamanan data meskipun ada kemajuan teknologi keamanan yang signifikan. Diskusikan strategi efektif untuk meningkatkan kesadaran keamanan karyawan dan menciptakan budaya keamanan yang kuat dalam organisasi. Bagaimana organisasi dapat mengukur efektivitas program kesadaran keamanan mereka?
5. Analisis bagaimana teknologi emerging seperti *artificial intelligence*, *Internet of Things*, dan *Blockchain* mengubah lanskap keamanan data. Apa ancaman keamanan unik yang ditimbulkan oleh setiap teknologi? Bagaimana organisasi harus mempersiapkan diri untuk mengatasi tantangan keamanan yang akan datang, khususnya dalam konteks komputasi kuantum dan kriptografi pasca-kuantum?

DAFTAR PUSTAKA

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: Preserving security and privacy. *Journal of Big Data*, 5(1), 1-12. **https://doi.org/10.1186/s40537-017-0110-7**

Ajisegiri, B. K., Oyewole, O. L., Binuyo, G., & Kappo-Abidemi, C. (2025). Development of frameworks for securing civil infrastructure information systems for building construction. *Eastern-European Journal of Enterprise Technologies*, 2313-8416, 004093. **https://doi.org/10.21303/2313-8416.2025.004093**

Gilbert, C., & Gilbert, M. (2025). Impact of general data protection regulation (GDPR) on data breach response strategies (DBRS). *International Journal of Research in Innovation and Sustainable Development*, 9(14), 0061. **https://doi.org/10.47772/ijriss.2025.914mg0061**

Golo, Z. A., Fahyudi, A., Ilyas, A. A., & Santika, T. (2023). Implementation of Electronic Medical Records at Primary Care in Semarang City Region: An Analysis of Individual and Organisational Determinants. Jurnal Penelitian Pendidikan IPA, 9(11), 9985–9991. **https://doi.org/10.29303/jppipa.v9i11.5627**

Ilyas, A. A., Golo, Z. A., Retnowati, & Saputra, J. D. (2023). Analisis Kesesuaian Variabel dan Meta Data Rekam Medis Elektronik : Studi Kasus pada Instalasi Rawat Jalan Rumah

Sakit X. Jurnal Rekam Medis dan Informasi Kesehatan, 6(2), 89–97. **https://doi.org/https://doi.org/10.31983/jrmik.v6i2.10640**

Ilyas, A. A., Golo, Z. A., Rosarini, A., Ningsih, K. P., Fahyudi, A., Hardiana, H., Oktoriani, E. N., Pratama, T. W. Y., Wahyuni, S., Saud, N. P. R., Wulandari, I., Hariyanto, S., & Sabran. (2025). Manajemen Rekam Medis Hybrid (H. Akbar (ed.)). CV. Media Sains Indonesia.

Ilyas, A. A., Golo, Z. A., Saputra, I. F., & Mulyana, B. P. (2025). Analisis Kebijakan Tanda Tangan Elektronik di Rumah Sakit Gigi dan Mulut Universitas Muhammadiyah Semarang. Jurnal Rekam Medis dan Informasi Kesehatan, 8(2), 122–130. **https://doi.org/https://doi.org/10.31983/jrmik.v8i2.13895**

Kandregula, P. K. (2025). Building secure projects: Cybersecurity principles for every stage. *International Journal of Scientific Research and Archive*, 15(2), 1460. **https://doi.org/10.30574/ijsra.2025.15.2.1460**

Narne, H., & Dholakia, S. (2025). Adaptive security model for cloud platforms based on information security and cryptographic protocols. *International Journal of Civil Engineering*, 2591. **https://doi.org/10.47941/ijce.2591**

Ogbodo, D. C., Awan, I., Cullen, A. J., & Zahrah, F. (2025). From regulation to reality: A framework to bridge the gap in digital

health data protection. *Electronics*, 14(13), 2629. **https://doi.org/10.3390/electronics14132629**

Ogunmolu, A. M. (2025). Enhancing data security in artificial intelligence systems: A cybersecurity and information governance approach. *Journal of Energy Research and Reviews*, 27(5), 1500. **https://doi.org/10.9734/jerr/2025/v27i51500**

Peraturan Menteri Kesehatan Nomor 24 tahun 2022 tentang Rekam Medis, Kementerian Kesehatan, Jakarta.

Pokhidnia, B. (2025). Ethics in information management: Personal data protection. *Eastern-European Professional Education*, 197, 212-216. **https://doi.org/10.30838/ep.197.212-216**

Rahman, M. M., Kshetri, N., Sayeed, S. A., & Rana, M. M. (2024). AssessITS: Integrating procedural guidelines and practical evaluation metrics for organizational IT and cybersecurity risk assessment. *Journal of Information Security*, 15(4), 32. **https://doi.org/10.4236/jis.2024.154032**

Wang, X., Bhuse, V., & Cheng, Y. (2025). A zero trust module for cybersecurity education. *Conference on Information Security and Software Innovation*, 12(1), 193. **https://doi.org/10.53735/cisse.v12i1.193**

Yeswanth, N., & Guntaka, R. (2026). Adaptive identity threat detection and response for enterprise cloud ecosystems. *Journal of Information Systems and*

Engineering Management, 11(1s), 14073. **https://doi.org/10.52783/jisem.v11i1s.14073**

BAB 4
RISIKO DAN ANCAMAN KEAMANAN DATA DI FASILITAS KESEHATAN

Natalia Kristiani, A.Md., S.KM, M.K.M

4.1 Jenis-Jenis Ancaman Keamanan Data di Fasilitas Kesehatan

4.1.1 Serangan Ransomware dan Data Breach

Serangan *ransomware* merupakan salah satu ancaman paling serius yang dihadapi oleh fasilitas kesehatan modern di era digitalisasi. Ancaman ini melibatkan perangkat lunak berbahaya yang mengenkripsi data penting sehingga tidak dapat diakses oleh pengguna yang sah, dan kemudian pelaku kejahatan siber meminta pembayaran untuk memberikan kunci dekripsi. Dalam konteks fasilitas kesehatan, serangan *ransomware* dapat menyebabkan gangguan operasional yang signifikan dan membahayakan nyawa pasien karena ketidakmampuan untuk mengakses catatan medis elektronik (*electronic health records* atau EHR). Penelitian menunjukkan bahwa serangan *ransomware* terus meningkat dengan dampak finansial yang mencapai jutaan dolar (Rahim et al., 2024). Selain itu, *data breach* atau pelanggaran data juga menjadi ancaman utama di mana data sensitif pasien bocor ke tangan yang tidak

berwenang, mengakibatkan risiko pencurian identitas dan kerugian finansial bagi pasien (Triplett, 2024).

4.1.2 Ancaman *Phishing* dan Serangan Sosial

Serangan *phishing* merupakan bentuk rekayasa sosial yang menargetkan karyawan fasilitas kesehatan dengan tujuan untuk mencuri kredensial akses atau informasi sensitif. Pelaku menggunakan email palsu, pesan singkat, atau komunikasi yang terlihat sah untuk membujuk karyawan agar mengungkapkan kata sandi atau mengakses tautan berbahaya. Penelitian terbaru menunjukkan bahwa sebagian besar pelanggaran data dalam sektor kesehatan disebabkan oleh faktor manusia, termasuk kerentanan terhadap serangan *phishing* dan kurangnya pelatihan keamanan yang memadai (Erukayenure et al., 2025). Serangan sosial ini sangat efektif karena memanfaatkan kelalaian manusia dan rendahnya kesadaran keamanan siber di kalangan petugas kesehatan yang sering kali terbebani dengan tugas klinis.

4.1.3 Ancaman dari Sistem Warisan dan Perangkat Medis yang Terhubung

Sistem warisan atau *legacy systems* yang masih digunakan oleh banyak fasilitas kesehatan sering kali memiliki kerentanan keamanan yang signifikan. Sistem-sistem ini dirancang pada era sebelum ancaman siber modern menjadi prioritas utama, sehingga tidak memiliki mekanisme pertahanan yang kuat. Penelitian menunjukkan bahwa sistem EHR warisan menjadi penyebab utama risiko keamanan siber di fasilitas kesehatan publik karena

ketidakmampuan mereka untuk menghadapi serangan canggih seperti *zero-day exploits* dan *malware* (Chuma, 2025). Sementara itu, perangkat medis yang terhubung ke jaringan (*Internet of Medical Things* atau IoMT) juga menimbulkan risiko keselamatan data yang baru. Perangkat-perangkat ini sering kali tidak dilengkapi dengan fitur keamanan bawaan, sehingga dapat dengan mudah diretas oleh penyerang untuk memanipulasi data pasien atau mengganggu fungsi perangkat (Shanmugam & Sivaraman, 2024).

4.1.4 Ancaman dari Insiden Keamanan Generasi Terbaru

Ancaman keamanan generasi terbaru mencakup penggunaan *artificial intelligence* (*AI*) untuk meningkatkan kecanggihan serangan siber. *Deepfake* dan pemalsuan suara AI menjadi ancaman yang berkembang pesat, di mana penyerang dapat membuat rekaman audio palsu untuk menyebarkan informasi menyesatkan atau melakukan penipuan yang menargetkan profesional kesehatan. Selain itu, integrasi teknologi AI generatif seperti *ChatGPT* dalam sistem kesehatan juga membawa risiko keamanan baru, termasuk kemungkinan paparan data sensitif melalui bug dalam perpustakaan *open-source* atau kerentanan dalam logika sistem (Sallam et al., 2024). Risiko-risiko ini menunjukkan bahwa lanskap ancaman keamanan data di fasilitas kesehatan terus berkembang dan memerlukan pembaruan berkelanjutan dalam strategi pertahanan.

4.2 Faktor-Faktor Kerentanan Sistem Kesehatan

4.2.1 Keterbatasan Sumber Daya dan Infrastruktur Keamanan yang Tidak Memadai

Fasilitas kesehatan, khususnya rumah sakit kecil dan pusat kesehatan masyarakat, sering menghadapi keterbatasan sumber daya finansial dan teknis untuk mengimplementasikan infrastruktur keamanan siber yang komprehensif. Penelitian menunjukkan bahwa sektor kesehatan mengalokasikan anggaran yang jauh lebih rendah untuk keamanan siber dibandingkan dengan industri lainnya (Qureshi & Koo, 2026). Keterbatasan ini mencakup kurangnya sistem enkripsi yang kuat, tidak adanya *firewall* canggih, dan tidak tersedianya solusi deteksi intrusi yang real-time. Akibatnya, fasilitas kesehatan menjadi target yang menarik bagi para penyerang siber karena kemudahan relatif untuk mengakses sistem mereka.

4.2.2 Kurangnya Kesadaran dan Pelatihan Karyawan

Faktor manusia merupakan elemen paling kritis dalam kerentanan keamanan data di fasilitas kesehatan. Meskipun ada kesadaran tentang pentingnya keamanan data, banyak karyawan kesehatan merasa kurang terlatih dan tidak terinformasi tentang penggunaan teknologi yang aman (Tikanmki, 2025). Kurangnya pelatihan keamanan yang berkelanjutan dan disesuaikan dengan kebutuhan spesifik petugas kesehatan menyebabkan mereka mudah jatuh korban terhadap serangan *phishing*, menggunakan kata sandi yang lemah, atau tidak mengikuti protokol keamanan yang

ditetapkan. Penelitian menunjukkan bahwa rendahnya kesadaran keamanan siber di kalangan profesional kesehatan tetap menjadi hambatan utama dalam mencapai postur keamanan yang kuat.

4.2.3 Kompleksitas Ekosistem Sistem Informasi Kesehatan

Ekosistem sistem informasi kesehatan modern sangat kompleks, melibatkan berbagai platform, perangkat, dan aplikasi yang saling terhubung. Integrasi EHR, perangkat IoMT, sistem cloud, dan aplikasi *telemedicine* menciptakan permukaan serangan yang luas, di mana setiap komponen dapat menjadi titik masuk bagi penyerang. Penelitian mengungkapkan bahwa komorbiditas antara berbagai sistem, ketergantungan pada vendor pihak ketiga, dan kurangnya standardisasi protokol keamanan meningkatkan kerentanan keseluruhan sistem (Ahmed et al., 2025). Selain itu, integrasi yang tidak aman antara sistem lama dan sistem baru sering kali menciptakan celah keamanan yang dapat dieksploitasi.

4.2.4 Kepatuhan Terhadap Regulasi dan Standar Keamanan yang Tidak Konsisten

Meskipun ada regulasi seperti *Health Insurance Portability and Accountability Act* (HIPAA) dan *General Data Protection Regulation* (GDPR) yang mengatur perlindungan data kesehatan, kepatuhan terhadap standar-standar ini tidak selalu konsisten di semua fasilitas kesehatan. Banyak organisasi kesehatan masih gagal memenuhi persyaratan kepatuhan penuh karena tantangan teknis, organisasional, dan finansial (Balogun, 2025). Standar keamanan NIST, enkripsi data, dan kontrol akses berbasis peran masih sering

tidak diimplementasikan dengan sempurna. Hal ini menciptakan celah regulasi yang dapat dieksploitasi oleh penyerang dan meningkatkan risiko penalti legal bagi organisasi kesehatan.

4.3 Dampak dan Konsekuensi Pelanggaran Keamanan Data

4.3.1 Dampak Langsung Terhadap Keselamatan Pasien

Pelanggaran keamanan data di fasilitas kesehatan memiliki dampak langsung yang serius terhadap keselamatan dan kesejahteraan pasien. Ketika data medis pasien diakses tanpa otorisasi atau diubah oleh penyerang, hal ini dapat menyebabkan kesalahan diagnosis dan pengobatan yang salah, yang pada gilirannya mengancam nyawa pasien. Serangan *ransomware* yang mengenkripsi EHR dapat mencegah akses ke informasi medis kritis selama prosedur darurat, memaksa dokter untuk mengandalkan ingatan atau catatan manual yang tidak lengkap. Penelitian menunjukkan bahwa insiden keamanan siber dapat menyebabkan gangguan operasional yang signifikan, kehilangan data, kegagalan sistem, dan penurunan kinerja sistem yang berdampak negatif pada kontinuitas perawatan kesehatan (Chuma, 2025).

4.3.2 Kerugian Finansial dan Reputasi Organisasi

Pelanggaran keamanan data mengakibatkan kerugian finansial yang sangat besar bagi fasilitas kesehatan. Biaya remediasi, biaya hukum, penggantian rugi kepada pasien, dan denda regulasi dapat mencapai jutaan dolar. Rata-rata biaya pelanggaran data dalam sektor kesehatan tahun 2023 mencapai 10,93 juta dolar

Amerika (Abdi et al., 2024). Selain kerugian finansial, pelanggaran data juga menyebabkan kerusakan reputasi yang signifikan, mengakibatkan kehilangan kepercayaan pasien dan kesulitan dalam merekrut karyawan berbakat. Organisasi kesehatan yang mengalami pelanggaran data seringkali membutuhkan waktu bertahun-tahun untuk memulihkan reputasi mereka di mata masyarakat.

4.3.3 Risiko Pencurian Identitas dan Penyalahgunaan Data Pribadi

Data kesehatan yang dilangar dapat digunakan untuk pencurian identitas dan penyalahgunaan finansial. Informasi pribadi pasien, nomor kartu kredit, dan riwayat medis yang bocor dapat dijual di pasar gelap (*dark market*) atau digunakan untuk membuka rekening bank palsu. Pencurian identitas medis juga dapat menyebabkan kesalahan dalam catatan kesehatan pasien, yang dapat mengakibatkan masalah kesehatan di masa depan. Penelitian menunjukkan bahwa jutaan catatan kesehatan telah dicuri melalui pelanggaran keamanan, menempatkan pasien pada risiko tinggi terhadap eksploitasi finansial dan dampak kesehatan jangka panjang (Triplett, 2024).

4.3.4 Gangguan Kontinuitas Layanan Kesehatan

Serangan siber terhadap infrastruktur kesehatan dapat menyebabkan gangguan serius dalam penyediaan layanan kesehatan. Ketika sistem informasi tidak berfungsi, rumah sakit harus beralih ke operasi manual yang tidak efisien, menyebabkan penundaan dalam diagnosis dan pengobatan. Perawatan darurat

dapat terhambat, prosedur elektif harus ditunda, dan koordinasi antarfasilitas kesehatan menjadi sulit. Kasus serangan *WannaCry* pada Layanan Kesehatan Nasional Inggris pada tahun 2017 menunjukkan bagaimana serangan siber dapat melumpuhkan sistem kesehatan yang luas, mengakibatkan ribuan pasien kehilangan akses ke layanan kesehatan penting (Rahim et al., 2024).

4.4 Strategi Mitigasi dan Perlindungan Data

4.4.1 Implementasi Teknologi Keamanan Canggih dan Enkripsi

Implementasi teknologi enkripsi yang kuat merupakan langkah fundamental dalam melindungi data kesehatan. Enkripsi data tingkat militer seperti *Advanced Encryption Standard* (AES) 256-bit harus diterapkan baik untuk data dalam transit maupun data dalam penyimpanan. Selain itu, organisasi kesehatan harus mengadopsi *multi-factor authentication* (MFA) untuk memverifikasi identitas pengguna dan mencegah akses tidak sah. Penelitian terbaru menunjukkan bahwa implementasi enkripsi berbasis quantum-resistant dan teknologi *Blockchain* dapat meningkatkan keamanan data kesehatan secara signifikan, memastikan integritas data dan memberikan audit trail yang tidak dapat diubah (Tiwo et al., 2025). Teknologi keamanan seperti *Zero Trust Architecture* (ZTA), di mana setiap pengguna dan perangkat harus diverifikasi terlepas dari lokasi mereka, juga terbukti efektif dalam mengurangi risiko akses tidak sah.

4.4.2 Program Pelatihan Kesadaran Keamanan Siber yang Komprehensif

Pelatihan keamanan siber yang berkelanjutan dan disesuaikan dengan kebutuhan spesifik berbagai peran dalam organisasi kesehatan sangat penting untuk membangun budaya keamanan yang kuat. Program pelatihan harus mencakup topik-topik seperti identifikasi serangan *phishing*, pembuatan kata sandi yang kuat, protokol keamanan data, dan respons terhadap insiden keamanan. Penelitian menunjukkan bahwa program pelatihan yang efektif dapat mengurangi risiko pelanggaran data yang disebabkan oleh faktor manusia hingga 60 persen (Tikanmki et al., 2025). Pelatihan harus dilakukan secara berkala dan disesuaikan dengan perkembangan ancaman keamanan terbaru, memastikan bahwa semua karyawan tetap terinformasi dan waspada terhadap risiko keamanan siber.

4.4.3 Governance, Manajemen Risiko, dan Kepatuhan Regulasi

Penerapan kerangka kerja *governance* yang kuat dengan manajemen risiko yang terstruktur menjadi kunci dalam menjaga keamanan data kesehatan. Organisasi kesehatan harus melakukan penilaian risiko secara berkala, mengidentifikasi kerentanan, dan mengembangkan rencana mitigasi yang komprehensif. Kepatuhan terhadap regulasi seperti HIPAA, GDPR, dan standar NIST harus menjadi prioritas utama, dengan audit reguler dan pembaruan kebijakan yang berkelanjutan (Komaragiri et al., 2025). Selain itu, pengembangan kebijakan insiden yang jelas dan rencana respons

darurat dapat membantu organisasi merespons pelanggaran keamanan dengan cepat dan meminimalkan dampak negatif.

4.4.4 Adopsi Teknologi Emerging untuk Perlindungan Data

Teknologi emerging seperti *artificial intelligence* (AI) dan *machine learning* (ML) dapat digunakan untuk meningkatkan deteksi ancaman dan respons insiden keamanan. Sistem deteksi anomali berbasis AI dapat mengidentifikasi perilaku pengguna yang tidak normal dan mencegah akses tidak sah secara real-time. Teknologi *Blockchain* juga menawarkan potensi untuk meningkatkan keamanan data kesehatan melalui sistem ledger terdistribusi yang tidak dapat diubah, memungkinkan verifikasi integritas data dan audit trail yang transparan (Pokharel et al., 2025). Implementasi *federated learning* memungkinkan organisasi kesehatan untuk berkolaborasi dalam pengembangan model keamanan tanpa membagikan data pasien yang sensitif, menciptakan sistem keamanan yang lebih kuat sambil menjaga privasi data (Tomar, 2025).

Latihan Soal

1. Jelaskan mengapa serangan *ransomware* merupakan ancaman yang paling berbahaya bagi fasilitas kesehatan dibandingkan dengan jenis serangan siber lainnya. Berikan contoh dampak nyata yang dapat terjadi.
2. Analisis hubungan antara kurangnya pelatihan karyawan dan meningkatnya risiko pelanggaran data di fasilitas kesehatan. Bagaimana organisasi kesehatan dapat mengatasi tantangan ini?
3. Bandingkan efektivitas antara teknologi enkripsi tradisional (AES 256-bit) dengan teknologi emerging seperti *Blockchain* dalam melindungi data kesehatan pasien.
4. Jelaskan bagaimana implementasi *Zero Trust Architecture* dapat meningkatkan keamanan sistem informasi kesehatan. Apa saja tantangan yang mungkin dihadapi dalam implementasinya?
5. Diskusikan peran *artificial intelligence* dan *machine learning* dalam deteksi ancaman keamanan siber di fasilitas kesehatan. Apa keterbatasan teknologi ini dan bagaimana cara mengatasinya?

DAFTAR PUSTAKA

Rahim, M. J., Rahim, M. I. I., Afroz, A., & Akinola, O. (2024). Cybersecurity threats in healthcare IT: Challenges, risks, and mitigation strategies. Journal of Artificial Intelligence and Information Systems, 6(1), 268. https://doi.org/10.60087/jaigs.v6i1.268

Chuma, K. (2025). *Legacy* electronic health record systems as culprit behind cybersecurity risks in public healthcare facilities of South Africa. International Journal of Healthcare Information Systems and Informatics, 25(7), 2532556. https://doi.org/10.1080/23779497.2025.2532556

Erukayenure, O., Bashir, H. A., Adekunbi, A., Abere, S. E., Okpan, O., & Guwa, A. A. (2025). Human factor vulnerabilities in healthcare cybersecurity: Mitigating insider threats in medical facilities. International Journal of Scientific Research and Advanced Engineering, 17(1), 2734. https://doi.org/10.30574/ijsra.2025.17.1.2734

Komaragiri, S. G., Alla, S., Duvall, T., Karahan, S., Bheesetty, N., & Chattu, V. (2025). A governance-centric framework for strengthening healthcare cybersecurity: A systems perspective. International Conference on Cyber Warfare and Security, 20(1), 3374. https://doi.org/10.34190/iccws.20.1.3374

Triplett, W. J. (2024). Cybersecurity vulnerabilities in healthcare: A threat to patient security. Current Issues in Technology and Justice, 2(1), 333. https://doi.org/10.53889/citj.v2i1.333

Qureshi, R., & Koo, I. (2026). A comprehensive survey of cybersecurity threats and data privacy issues in healthcare systems. Applied Sciences, 16(3), 1511. https://doi.org/10.3390/app16031511

Sallam, M., Al-Mahzoum, K., & Sallam, M. (2024). Generative artificial intelligence and cybersecurity risks: Implications for healthcare security based on real-life incidents. Medical Journal of Artificial Intelligence and Healthcare, 2024(019). https://doi.org/10.58496/mjaih/2024/019

Ahmed, Z., Osifowokan, A. S., Filani, A., & Donkor, A. A. (2025). Comprehensive analysis of cyber attacks and data breaches in the US health sector: Identifying vulnerabilities and developing proactive defense strategies. CESJ – Computer Science International Research Journal, 6(2), 1833. https://doi.org/10.51594/csitrj.v6i2.1833

Tikanmki, I., Blek, T., Niskakangas, J., & Varamki, K. (2025). Enhancing cybersecurity in healthcare: The KyberSoTe project's approach to mitigating cyber threats. European Conference on Cyber Warfare and Security, 24(1), 3477. https://doi.org/10.34190/eccws.24.1.3477

Pokharel, B. P., Kshetri, N., Sharma, S. R., & Paudel, S. (2025). blockHealthSecure: Integrating *Blockchain* and

cybersecurity in post-pandemic healthcare systems. Information, 16(2), 133. https://doi.org/10.3390/info16020133

BAB 5
PRINSIP PERLINDUNGAN DATA DALAM SISTEM INFORMASI KESEHATAN

Setya Wijayanta, S.T.,M.Kes

5.1 Fondasi dan Prinsip Dasar Perlindungan Data dalam Sistem Informasi Kesehatan

5.1.1 Pengertian dan Pentingnya Perlindungan Data Kesehatan

Perlindungan data dalam sistem informasi kesehatan merupakan aspek krusial dalam penyelenggaraan layanan kesehatan modern yang berorientasi pada era digital. Sistem informasi kesehatan, atau *Health Information Systems* (HIS), memiliki tanggung jawab utama untuk menyimpan, mengelola, dan membagikan informasi pasien dengan aman dan terpercaya. Data kesehatan merupakan kategori khusus dari data pribadi yang sangat sensitif karena mengandung informasi medis, genetik, dan biometrik yang dapat berdampak signifikan terhadap privasi dan kesejahteraan individu (Shojaei et al., 2024).

Dalam konteks transformasi digital, perlindungan data kesehatan tidak hanya sekadar tanggung jawab etis, tetapi juga merupakan kewajiban hukum yang ketat. *Health Informatics* telah merevolusi cara data pasien dikumpulkan, dikelola, dan

dimanfaatkan untuk meningkatkan kualitas layanan kesehatan. Namun, seiring dengan semakin terintegranya sistem digital dalam praktik kesehatan, kekhawatiran mengenai privasi dan keamanan data semakin meningkat. Ancaman-ancaman seperti akses tidak sah, serangan siber, dan penyalahgunaan data menunjukkan perlunya pendekatan komprehensif terhadap perlindungan informasi kesehatan (Triplett, 2024).

5.1.2 Tiga Pilar Utama Keamanan Data: Confidentiality, Integrity, dan Availability

Prinsip dasar keamanan informasi kesehatan dibangun atas tiga pilar utama yang sering disingkat sebagai CIA: *Confidentiality* (Kerahasiaan), *Integrity* (Integritas), dan *Availability* (Ketersediaan). Kerahasiaan memastikan bahwa informasi kesehatan hanya dapat diakses oleh pihak yang berwenang. Prinsip ini berfungsi untuk mencegah akses tidak sah dan penyalahgunaan data pribadi pasien. Integritas menjamin bahwa data kesehatan tidak mengalami perubahan, penghapusan, atau pemalsuan yang tidak sah. Ketersediaan memastikan bahwa data kesehatan dapat diakses dan digunakan oleh pihak yang berhak pada waktu yang diperlukan untuk memberikan layanan kesehatan yang optimal (Shojaei et al., 2024).

Ketiga pilar ini bekerja secara sinergis untuk menciptakan lingkungan yang aman bagi pengelolaan data kesehatan. Dalam praktik nyata, implementasi ketiga prinsip tersebut memerlukan kombinasi dari berbagai strategi teknis, organisasi, dan prosedural.

Organisasi kesehatan harus mengembangkan kebijakan yang jelas mengenai penanganan data, melakukan pelatihan berkelanjutan kepada staf, dan menerapkan teknologi keamanan yang mutakhir (Bhaskar et al., 2023).

5.1.3 Hak dan Kewajiban Subjek Data dalam Perlindungan Informasi Kesehatan

Subjek data, dalam hal ini pasien, memiliki serangkaian hak fundamental yang harus dilindungi. Hak-hak ini mencakup hak untuk mengetahui bagaimana data pribadi mereka digunakan, hak untuk mengakses data mereka sendiri, hak untuk merekti atau melengkapi data yang tidak akurat, dan hak untuk menghapus data mereka dalam keadaan tertentu. Selain itu, pasien memiliki hak untuk memberikan persetujuan yang terinformasi sebelum data kesehatan mereka diproses atau dibagikan dengan pihak ketiga.

Sebaliknya, organisasi kesehatan sebagai pengontrol data memiliki kewajiban untuk memastikan bahwa data pasien ditangani dengan cara yang bertanggung jawab dan etis. Kewajiban ini meliputi implementasi langkah-langkah keamanan yang layak, melakukan penilaian dampak privasi, mempertahankan catatan pemrosesan data, dan melaporkan pelanggaran data ke otoritas yang berwenang. Keseimbangan antara hak pasien dan kewajiban organisasi merupakan inti dari perlindungan data kesehatan yang efektif (Jurczuk & Suprunowicz, 2024).

5.1.4 Etika dan Transparansi dalam Pengelolaan Data Kesehatan

Etika merupakan fondasi yang tidak terpisahkan dari perlindungan data kesehatan. Prinsip-prinsip etika dalam pengelolaan data kesehatan mencakup otonomi individu (*autonomy*), kebajikan (*beneficence*), tidak merugikan (*non-maleficence*), dan keadilan (*justice*). Otonomi berarti menghormati hak pasien untuk membuat keputusan tentang data mereka sendiri. Kebajikan mengharuskan organisasi kesehatan untuk menggunakan data dengan cara yang menguntungkan pasien dan masyarakat. Tidak merugikan berarti meminimalkan risiko kerugian dari penggunaan data. Keadilan memastikan bahwa manfaat dan beban dari penggunaan data didistribusikan secara adil di antara berbagai kelompok.

Transparansi merupakan aspek penting untuk membangun kepercayaan pasien terhadap sistem informasi kesehatan. Organisasi kesehatan harus secara terang-terangan mengkomunikasikan bagaimana data pasien dikumpulkan, diproses, disimpan, dan digunakan. Informasi ini harus disajikan dengan cara yang mudah dipahami oleh pasien awam. Transparansi juga mencakup penyediaan jalur yang jelas bagi pasien untuk mengajukan keberatan atau keluhan mengenai penanganan data mereka (Hamdan et al., 2024).

5.2 Regulasi dan Kerangka Kerja Hukum Perlindungan Data Kesehatan

5.2.1 GDPR dan Penerapannya dalam Sistem Informasi Kesehatan

General Data Protection Regulation (GDPR) merupakan regulasi perlindungan data yang paling komprehensif di dunia, yang diterapkan di Uni Eropa dan memiliki jangkauan global. GDPR menetapkan standar ketat untuk pengumpulan, pemrosesan, dan penyimpanan data pribadi, termasuk data kesehatan. Regulasi ini memberikan wewenang kepada individu dengan kontrol yang lebih besar atas data pribadi mereka dan menetapkan aturan yang jelas bagi organisasi yang menangani data tersebut.

Dalam konteks sistem informasi kesehatan, GDPR memiliki implikasi signifikan. Pertama, GDPR mengharuskan organisasi kesehatan untuk memiliki dasar hukum yang jelas (*legal basis*) sebelum memproses data kesehatan. Kedua, regulasi ini mewajibkan implementasi prinsip *privacy by design*, yang berarti perlindungan privasi harus dibangun sejak awal dalam sistem informasi. Ketiga, GDPR memerlukan penilaian dampak privasi (*Data Protection Impact Assessment* atau DPIA) untuk operasi pemrosesan data yang berisiko tinggi. Keempat, organisasi harus mematuhi hak-hak data subjek, termasuk hak untuk dilupakan (*right to be forgotten*) (Shah, 2023).

Studi menunjukkan bahwa standar *OpenEHR*, yang merupakan standar untuk sistem catatan kesehatan elektronik, dapat

membantu organisasi kesehatan mencapai kepatuhan terhadap GDPR. Namun, penelitian juga mengungkapkan bahwa tidak semua aspek dari standar *OpenEHR* sepenuhnya sejalan dengan persyaratan GDPR, menyoroti pentingnya membangun keamanan sejak awal dalam pengembangan sistem informasi kesehatan.

5.2.2 HIPAA dan Persyaratan Keamanan di Amerika Serikat

Health Insurance Portability and Accountability Act (HIPAA) adalah undang-undang fundamental di Amerika Serikat yang mengatur perlindungan informasi kesehatan yang dilindungi (*Protected Health Information* atau PHI). HIPAA terdiri dari beberapa komponen utama, termasuk *Privacy Rule*, *Security Rule*, dan *Breach Notification Rule*. *Privacy Rule* mengatur penggunaan dan pengungkapan PHI oleh entitas yang ditentukan. *Security Rule* melengkapi *Privacy Rule* dengan mewajibkan entitas untuk mengimplementasikan perlindungan fisik, teknis, dan administratif untuk melindungi privasi PHI (Abbasi & Smith, 2024).

HIPAA menetapkan standar ketat untuk akses, penyimpanan, dan transmisi data kesehatan. Organisasi kesehatan yang mematuhi HIPAA harus melakukan penilaian risiko keamanan secara berkala, mengimplementasikan enkripsi data, mempertahankan kontrol akses berbasis peran, dan memastikan audit trail yang komprehensif. Pelanggaran HIPAA dapat mengakibatkan denda signifikan dan kerusakan reputasi bagi organisasi kesehatan (Yowetu et al., 2024).

5.2.3 Peraturan Data Perlindungan Data Lokal dan Regional

Selain GDPR dan HIPAA, berbagai yurisdiksi telah mengembangkan peraturan perlindungan data mereka sendiri. Di Indonesia, terdapat Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menetapkan prinsip-prinsip transparansi, keamanan, dan akuntabilitas dalam perlindungan data, selanjutnya, UU No. 17 Tahun 2023 tentang Kesehatan (Pasal 276) menjamin kerahasiaan data individu yang hanya boleh diakses pihak berwenang, sementara PMK No. 24 Tahun 2022 tentang Rekam Medis mewajibkan fasyankes menerapkan RME dengan pengendalian akses berbasis kewenangan, audit trail, serta jaminan keamanan, kerahasiaan, integritas, dan ketersediaan data. Peraturan ini sangat relevan untuk organisasi kesehatan yang menangani data sensitif seperti informasi kesehatan, data biometrik, dan data genetik, serta semua selaras mendukung interoperabilitas yang aman ke dalam platform SatuSehat.

Di negara-negara lain seperti Amerika Serikat, terdapat juga *California Consumer Privacy Act* (CCPA) yang memberikan konsumen hak lebih besar atas data pribadi mereka. Organisasi kesehatan yang melayani pasien di berbagai yurisdiksi harus memahami dan mematuhi berbagai peraturan yang berlaku di setiap wilayah (Yowetu et al., 2024).

5.2.4 Keselarasan dan Harmonisasi Regulasi Internasional

Kompleksitas lingkungan regulasi global menciptakan tantangan bagi organisasi kesehatan multinasional atau yang

melayani pasien internasional. Berbagai peraturan memiliki persyaratan yang berbeda, dan dalam beberapa kasus, saling bertentangan. Untuk mengatasi tantangan ini, organisasi harus mengadopsi pendekatan yang proaktif dan adaptif terhadap kepatuhan data privacy.

Perbandingan antara GDPR dan HIPAA menunjukkan bahwa meskipun kedua regulasi memiliki tujuan serupa untuk melindungi privasi data kesehatan, mereka memiliki perbedaan signifikan dalam pendekatan dan persyaratan. GDPR mengadopsi pendekatan berbasis hak yang lebih komprehensif, sementara HIPAA lebih fokus pada sektor-sektor tertentu. Organisasi yang beroperasi secara global harus mengadopsi standar yang paling ketat untuk memastikan kepatuhan di semua yurisdiksi (Jurczuk & Suprunowicz, 2024).

5.3 Teknologi Perlindungan Data dalam Sistem Informasi Kesehatan

5.3.1 Enkripsi Data: Enkripsi Saat Disimpan dan Dalam Transmisi

Enkripsi merupakan salah satu teknologi paling penting dalam perlindungan data kesehatan. Enkripsi berfungsi untuk mengubah data yang dapat dibaca menjadi format yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai. Teknologi enkripsi diterapkan pada dua titik kritis: data saat disimpan (*at rest*) dan data dalam perjalanan (*in transit*).

Enkripsi data saat disimpan memastikan bahwa informasi kesehatan yang tersimpan di server, basis data, atau media penyimpanan lainnya tidak dapat diakses oleh pihak yang tidak berwenang. Standar enkripsi seperti *Advanced Encryption Standard* (AES) dengan panjang kunci 256-bit atau lebih telah menjadi praktik standar dalam industri kesehatan. Enkripsi data dalam transmisi menggunakan protokol seperti *Hypertext Transfer Protocol Secure* (HTTPS) dan *Transport Layer Security* (TLS) untuk melindungi data yang dikirimkan melalui jaringan (Basha et al., 2024).

Perkembangan terbaru dalam teknologi enkripsi mencakup penggunaan enkripsi homomorfik, yang memungkinkan perhitungan dilakukan pada data terenkripsi tanpa perlu mendekripsi data terlebih dahulu. Teknologi ini memiliki potensi signifikan untuk memungkinkan analisis data kesehatan yang aman sambil mempertahankan privasi pasien (Aishwarya & Sriramya, 2025).

5.3.2 *Federated Learning* dan Teknik Pengawetan Privasi

Federated Learning (FL) merupakan paradigma pembelajaran mesin yang memungkinkan model dilatih secara terdistribusi tanpa perlu mengumpulkan data sensitif di lokasi pusat. Dalam konteks kesehatan, FL memungkinkan institusi kesehatan yang berbeda untuk berkolaborasi dalam pengembangan model pembelajaran mesin tanpa berbagi data pasien raw dengan pihak lain. Setiap institusi melatih model secara lokal menggunakan data

mereka sendiri, dan hanya pembaruan model yang dibagikan dengan server pusat (Wani & Can, 2025).

Teknologi pengawetan privasi lainnya yang sering digunakan bersamaan dengan FL termasuk *Differential Privacy* (DP) dan *Secure Multi-Party Computation* (SMPC). *Differential Privacy* menambahkan kebisingan yang terkontrol ke hasil untuk memastikan bahwa tidak mungkin untuk menyimpulkan informasi tentang individu tertentu dari hasil analisis. SMPC memungkinkan beberapa pihak untuk melakukan perhitungan bersama pada data terpisah mereka tanpa mengungkapkan data individual (Ts, 2025).

Kombinasi dari FL, DP, dan SMPC telah terbukti menjadi solusi yang efektif untuk memenuhi persyaratan perlindungan data dalam penelitian medis sambil mempertahankan kegunaan data untuk tujuan analitik dan pembelajaran mesin (G et al., 2025).

5.3.3 *Blockchain* untuk Transparansi dan Integritas Data

Teknologi *Blockchain* menawarkan solusi unik untuk perlindungan data kesehatan melalui karakteristik desentralisasi, ketidakubahan, dan transparansi. Dalam sistem informasi kesehatan berbasis *Blockchain*, setiap transaksi atau perubahan data dicatat dalam blok yang dikriptografi dan terhubung dengan blok sebelumnya. Struktur ini memastikan bahwa data tidak dapat diubah tanpa dideteksi (Kunal et al., 2024).

Blockchain juga memungkinkan implementasi *smart contracts*, yaitu program otomatis yang dapat menegakkan

persetujuan pasien dan kebijakan privasi. Smart contract dapat secara otomatis membatasi akses ke data kesehatan berdasarkan aturan yang telah ditetapkan sebelumnya. Sistem *Blockchain* dapat menghasilkan audit trail yang komprehensif dan transparan, memudahkan pemantauan kepatuhan terhadap peraturan perlindungan data (Barbaria et al., 2025).

Namun, implementasi *Blockchain* dalam sistem informasi kesehatan juga menghadapi tantangan, termasuk masalah skalabilitas, konsumsi energi yang tinggi, dan kompleksitas teknis. Penelitian menunjukkan bahwa meskipun *Blockchain* memiliki potensi besar, masih diperlukan pengembangan lebih lanjut untuk mencapai adopsi yang luas dalam praktik kesehatan sehari-hari (Nasar et al., 2025).

5.3.4 Sistem Deteksi Ancaman dan Respons Insiden Real-Time

Sistem deteksi ancaman menggunakan kecerdasan buatan (*Artificial Intelligence* atau AI) dan pembelajaran mesin (*Machine Learning* atau ML) untuk mengidentifikasi pola perilaku yang mencurigakan atau tidak normal dalam sistem informasi kesehatan. Sistem ini dapat mendeteksi akses tidak sah, percobaan pelanggaran data, dan aktivitas berbahaya lainnya secara real-time (V et al., 2025).

Sistem respons insiden dirancang untuk merespons pelanggaran keamanan dengan cepat dan efektif. Respons yang cepat dapat meminimalkan kerusakan dari pelanggaran data dan membantu organisasi kesehatan memenuhi persyaratan notifikasi

pelanggaran dalam peraturan seperti GDPR dan HIPAA. Kombinasi dari deteksi ancaman proaktif dan respons insiden yang efisien menciptakan postur keamanan yang kuat untuk sistem informasi kesehatan (Arefin & Simcox, 2024).

5.4 Implementasi dan Tata Kelola Perlindungan Data dalam Sistem Informasi Kesehatan

5.4.1 *Privacy by Design* dan Penilaian Dampak Privasi

Privacy by Design (PbD) merupakan pendekatan yang mengintegrasikan perlindungan privasi dalam setiap tahap pengembangan sistem informasi kesehatan, dari perencanaan awal hingga peluncuran dan pemeliharaan berkelanjutan. Prinsip-prinsip PbD mencakup proaktivitas, privasi sebagai nilai default, visibilitas dan transparansi, serta perlindungan pengguna akhir (V et al., 2025).

Penilaian Dampak Privasi (*Data Protection Impact Assessment* atau DPIA) merupakan alat penting dalam implementasi PbD. DPIA adalah evaluasi sistematis dari risiko perlindungan data yang mungkin timbul dari operasi pemrosesan data tertentu. Melalui DPIA, organisasi kesehatan dapat mengidentifikasi risiko potensial dan mengimplementasikan langkah-langkah mitigasi sebelum sistem diluncurkan (Frempong et al., 2024).

Implementasi PbD memerlukan kolaborasi erat antara berbagai stakeholder, termasuk profesional kesehatan, spesialis keamanan informasi, dan petugas perlindungan data. Pendekatan holistik ini memastikan bahwa perlindungan data diintegrasikan

dengan efektif ke dalam operasi klinis sehari-hari (Akter & Sanam, 2025).

5.4.2 Kontrol Akses Berbasis Peran dan Manajemen Identitas

Kontrol Akses Berbasis Peran (*Role-Based Access Control* atau RBAC) merupakan mekanisme keamanan fundamental dalam sistem informasi kesehatan. RBAC membatasi akses ke data kesehatan berdasarkan peran dan tanggung jawab pengguna. Misalnya, perawat mungkin memiliki akses ke catatan pasien di unit tempat mereka bekerja, sementara administrator sistem mungkin memiliki akses yang lebih luas untuk tujuan manajemen sistem (Shojaei et al., 2024).

Manajemen identitas yang kuat adalah prasyarat untuk efektivitas RBAC. Sistem manajemen identitas harus memastikan bahwa identitas pengguna diverifikasi secara akurat, peran pengguna diperbarui secara tepat waktu ketika ada perubahan tanggung jawab, dan akses dibatalkan dengan segera ketika pengguna meninggalkan organisasi. Teknologi autentikasi multi-faktor dan sistem manajemen akses istimewa juga merupakan komponen penting dari keamanan akses (Frimpong et al., 2025).

5.4.3 Audit Trail, Logging, dan Pemantauan Berkelanjutan

Audit trail yang komprehensif merekam semua aktivitas yang terkait dengan akses dan penggunaan data kesehatan. Setiap akses ke catatan pasien, setiap modifikasi data, dan setiap pembagian data dengan pihak ketiga harus dicatat. Informasi yang dicatat dalam audit trail mencakup siapa yang melakukan tindakan, kapan tindakan

dilakukan, apa yang dilakukan, dan apakah tindakan tersebut berhasil.

Logging yang efektif memungkinkan organisasi kesehatan untuk mendeteksi aktivitas mencurigakan, menyelidiki insiden keamanan, dan membuktikan kepatuhan terhadap peraturan. Dalam era big data, manajemen logs yang efisien memerlukan penggunaan teknologi advanced analytics dan machine learning untuk mengidentifikasi pola anomali (M, 2024).

Pemantauan berkelanjutan memastikan bahwa sistem perlindungan data tetap efektif seiring waktu. Organisasi kesehatan harus secara rutin meninjau kebijakan perlindungan data, mengevaluasi keefektifan kontrol keamanan, dan melakukan pembaruan untuk mengatasi ancaman baru (Sardana et al., 2025).

5.4.4 Pelatihan, Kesadaran, dan Budaya Keamanan

Faktor manusia memainkan peran penting dalam kesuksesan perlindungan data. Pelatihan keamanan informasi yang komprehensif untuk semua staf kesehatan merupakan investasi penting dalam menciptakan budaya keamanan yang kuat. Pelatihan harus mencakup topik-topik seperti pengenalan serangan phishing, praktik manajemen kata sandi yang aman, protokol keamanan data, dan prosedur respons insiden (Hamdan et al., 2024).

Kesadaran keamanan yang tinggi di kalangan staf kesehatan dapat secara signifikan mengurangi risiko pelanggaran data yang disebabkan oleh kesalahan manusia atau kelalaian. Program kesadaran harus disesuaikan dengan peran spesifik pengguna dan

harus diperbarui secara berkala untuk mencerminkan ancaman baru dan praktik terbaik. Budaya keamanan yang kuat di organisasi kesehatan berarti bahwa perlindungan data bukan hanya tanggung jawab departemen keamanan informasi, tetapi merupakan tanggung jawab bersama yang dianut oleh semua anggota organisasi (Hamdan et al., 2024).

5.5 Zero Trust untuk Keamanan Electronic Medical Record (EMR)

5.5.1 Mengapa Zero Trust untuk Keamanan EMR

Seiring meningkatnya adopsi Electronic Medical Record (EMR) di rumah sakit dan puskesmas, pola akses data pasien menjadi jauh lebih kompleks: dokter mengakses dari ruang rawat inap, perawat dari nurse station, farmasi dari loket obat, radiologi dari ruang pemeriksaan, bahkan ada akses jarak jauh untuk telemedicine dan konsultasi antar fasilitas. Lingkungan yang dinamis ini membuat model keamanan lama yang hanya mengandalkan "tembok" jaringan internal (*firewall*) tidak lagi cukup.

Zero Trust hadir sebagai pendekatan baru yang berprinsip bahwa tidak ada satu pun pengguna atau perangkat yang otomatis dipercaya hanya karena berada di "dalam" jaringan rumah sakit. Setiap permintaan akses ke data rekam medis harus selalu diverifikasi, dibatasi sesuai kewenangan, dan diawasi. Dengan cara ini, risiko kebocoran data pasien, penyalahgunaan akses oleh orang

dalam, dan penyebaran serangan seperti ransomware dapat ditekan secara lebih sistematis (Yadav, N., 2024).

Dalam konteks EMR, penerapan Zero Trust membantu menjawab beberapa tantangan utama, seperti:

- Akses tidak sah terhadap rekam medis karena akun dibagi-bagi atau dicuri.
- Kebocoran data pasien melalui perangkat yang hilang atau koneksi jarak jauh yang tidak aman.
- Penyalahgunaan hak oleh internal (*insider threat*), misalnya melihat data selebritas tanpa alasan klinis.
- Serangan malware dan ransomware yang menyebar dari satu komputer ke seluruh jaringan rumah sakit.

5.5.2 Konsep Dasar Zero Trust dalam EMR

Secara sederhana, Zero Trust dapat diringkas dalam prinsip "never trust, always verify". Artinya, setiap permintaan akses terhadap EMR harus selalu:

- Diautentikasi: sistem memastikan siapa yang sedang mengakses.
- Diotorisasi: sistem mengecek apakah orang tersebut berhak mengakses data atau fungsi tertentu.
- Dilindungi: seluruh komunikasi dan penyimpanan data dilakukan secara terenkripsi.

Pada praktiknya, hal ini berarti:

- Dokter, perawat, petugas rekam medis, dan staf administrasi tidak otomatis mendapatkan akses luas hanya karena menggunakan komputer di dalam jaringan rumah sakit.

- Kebijakan akses mempertimbangkan identitas, peran, unit kerja, lokasi, perangkat, dan konteks (misalnya jam kerja, pola akses).
- Semua aktivitas yang berkaitan dengan akses dan perubahan data pasien direkam dalam log dan dipantau secara aktif.

5.5.3 Model Tradisional vs Zero Trust di Lingkungan EMR

Untuk mempermudah pemahaman, perbedaan model tradisional dan Zero Trust dalam EMR dapat dilihat sebagai berikut.

Model Keamanan Tradisional (Perimeter-Based)

- Bertumpu pada firewall dan jaringan internal rumah sakit.
- Setelah terhubung ke jaringan internal, pengguna sering mendapat akses luas ke berbagai sistem.
- Jika satu akun atau satu komputer berhasil ditembus, penyerang bisa bergerak ke sistem lain tanpa banyak hambatan.
- Cukup efektif di era ketika sistem masih terpusat, tidak banyak akses dari luar, dan tidak ada integrasi luas.

Model Zero Trust

- Tidak ada akses otomatis hanya karena berada di jaringan internal.
- Setiap akses ke modul EMR (rawat jalan, rawat inap, farmasi, laboratorium, radiologi, keuangan) divalidasi kembali sesuai identitas dan peran.
- Menggunakan kontrol akses berbasis peran (Role-Based Access Control/RBAC) serta, bila perlu, atribut (jam kerja, lokasi, jenis perangkat).

- Aktivitas pengguna diawasi secara berkelanjutan melalui audit trail dan sistem pemantauan.

Model Zero Trust sangat relevan untuk:

- EMR berbasis web yang diakses dari berbagai unit dan perangkat.
- Integrasi dengan laboratorium, farmasi, BPJS(E-Claim), dan sistem rujukan/telemedicine.
- Akses mobile oleh tenaga kesehatan (tablet visite, smartphone dokter on-call).

5.5.4 Komponen Utama Zero Trust pada Sistem EMR

Implementasi Zero Trust di EMR dapat dipecah menjadi beberapa komponen praktis, agar lebih mudah direncanakan dan dijalankan.

1) Identity and Access Management (IAM) pada EMR

- Setiap individu (dokter, perawat, PMIK, admin TI, billing) mempunyai akun sendiri, tidak boleh ada akun bersama.
- Prinsip least privilege: hak akses diberikan seperlunya untuk menjalankan tugas, tidak lebih.
- Multi-Factor Authentication (MFA) digunakan untuk akses sensitif, misalnya dokter yang mengakses dari luar fasilitas atau admin yang mengelola konfigurasi sistem.

2) Role-Based Access Control (RBAC)

- Dokter hanya dapat mengakses data pasien yang ditanganinya atau yang menjadi tanggung jawab unitnya.
- Petugas billing hanya melihat informasi administratif dan finansial, tidak bisa membuka catatan klinis detail.

- Petugas rekam medis memiliki hak sesuai ketentuan hukum: pengelolaan berkas, koreksi identitas, pengarsipan, namun tidak mengubah diagnosis yang sudah ditetapkan dokter.

3) Perlindungan Data (Data Encryption)

- Data pasien di database EMR dienkripsi ketika disimpan (*encryption at rest*), sehingga bila server dicuri atau disalin tanpa izin, data tetap tidak mudah dibaca.
- Semua komunikasi antar klien dan server EMR, termasuk akses web dan API, menggunakan protokol aman seperti HTTPS/TLS (*encryption in transit*).
- Kunci enkripsi dikelola secara aman dengan prosedur yang jelas dan terbatas hanya bagi pihak yang berwenang.

4) Pemantauan Berkelanjutan dan Audit Trail

- Setiap akses, perubahan, dan pengambilan data pasien dicatat dalam log: siapa, kapan, dari mana, dan apa yang diakses atau diubah.
- Log diperiksa secara berkala untuk mendeteksi pola tidak wajar, misalnya akses massal di luar jam kerja atau akses berulang terhadap rekam medis tokoh publik.
- Organisasi memiliki mekanisme tindak lanjut bila ditemukan indikasi penyalahgunaan, termasuk proses investigasi dan pemberian sanksi.

5) Segmentasi Jaringan (Network Segmentation)

- Server EMR ditempatkan di segmen jaringan yang terpisah dari jaringan umum (misalnya Wi-Fi tamu) atau komputer non-medis.

- Modul klinis (rekam medis, farmasi, lab) disegmentasi dari sistem administratif umum, sehingga serangan pada satu area tidak otomatis menjalar ke area lain.
- Akses dari luar (telemedicine, remote support) dibatasi melalui VPN, firewall, dan kontrol tambahan.

6) Teknologi Pendukung

Beberapa teknologi yang sering digunakan untuk mendukung Zero Trust pada EMR antara lain:

- Single Sign-On (SSO) untuk menyatukan otentikasi ke berbagai aplikasi klinis.
- MFA untuk mencegah penyalahgunaan password.
- Intrusion Detection/Prevention System (IDS/IPS) untuk mendeteksi pola serangan pada jaringan.
- Web Application Firewall (WAF) untuk melindungi aplikasi EMR berbasis web.
- Endpoint security (antivirus/EDR) pada komputer klinik.
- Data Loss Prevention (DLP) untuk mengawasi dan mencegah penyalinan data pasien secara tidak sah.
- SIEM (Security Information and Event Management) untuk mengumpulkan dan menganalisis log keamanan secara terpusat.

5.5.5 Tantangan dan Strategi Penerapan Zero Trust

Menerapkan Zero Trust bukan tanpa tantangan, terutama di fasilitas pelayanan kesehatan (fasyankes) dengan sumber daya terbatas atau sistem informasi yang sudah lama.

Beberapa tantangan umum:

- Kompleksitas implementasi dan potensi mengganggu alur kerja bila perubahan dilakukan mendadak.
- SIMRS lama yang belum mendukung RBAC granular, audit trail lengkap, atau MFA.
- Biaya awal untuk infrastruktur keamanan dan pelatihan staf.
- Resistensi budaya kerja karena tenaga kesehatan merasa akses menjadi lebih “ribet” dan memperlambat proses pelayanan.
- Keterbatasan tim TI di rumah sakit kecil.

Strategi yang dapat dilakukan:

- Mulai dari modul paling kritis (misalnya EHR utama dan akses dokter) sebelum meluas ke semua sistem.
- Libatkan tenaga kesehatan sejak awal dalam perancangan kebijakan, sehingga desain kontrol tidak menghambat pelayanan.
- Lakukan pelatihan singkat dan berulang tentang mengapa Zero Trust penting untuk melindungi pasien dan reputasi rumah sakit.
- Susun rencana bertahap, termasuk pemutakhiran sistem lama secara terencana (phased migration).

Latihan Soal

1. Jelaskan mengapa ketiga pilar keamanan informasi (CIA - Confidentiality, Integrity, dan Availability) sama pentingnya dalam sistem informasi kesehatan, dan berikan contoh konkret dari setiap pilar dalam konteks data pasien.
2. Bandingkan dan kontraskan pendekatan GDPR dan HIPAA dalam perlindungan data kesehatan. Mengapa organisasi kesehatan multinasional harus memahami perbedaan ini?
3. Diskusikan peran teknologi enkripsi dan federated learning dalam memungkinkan inovasi kesehatan digital sambil mempertahankan privasi pasien.
4. Jelaskan konsep *Privacy by Design* dan mengapa penting untuk mengintegrasikan prinsip ini dari awal pengembangan sistem informasi kesehatan daripada menambahkannya kemudian.
5. Analisis peran budaya keamanan organisasi dan pelatihan staf dalam pencegahan pelanggaran data kesehatan. Apa yang dapat dilakukan organisasi untuk membangun budaya keamanan yang kuat?

DAFTAR PUSTAKA

Abuuzzam, A. A., Al-Qahtani, S., SalahMohammed, H., Alshhry, R., Abdullah, A., Hadadi, Alotaibi, E. T., Abuazzam, A. A., Othaibi, S. S. A., Rasheed, H., Kumait, M., Ali, A., Dighriri, A., Bader, S. N., Ibrahim, A., Althurwi, H., Abulrazaq, A., Mohmmed, A., Ghalib, N., & Haweidi, B. (2024). The human firewall imperative: A narrative review of interprofessional collaboration for cybersecurity in patient-centric digital healthcare. *Journal Name*, 12(4), 337. **https://doi.org/10.64483/202412337**

Arefin, S., & Simcox, M. (2024). AI-driven solutions for safeguarding healthcare data: Innovations in cybersecurity. *International Business Research*, 17(6), 74. **https://doi.org/10.5539/ibr.v17n6p74**

Akter, S., & Sanam, T. F. (2025). A *Blockchain* framework for secure healthcare data management using role-based access control and smart contracts. In *Proceedings of the IEEE Conference* (pp. 11013162). **https://doi.org/10.1109/ECCE64574.2025.11013162**

Basha, C. B., Murugan, K., Suresh, T., SrirengaNachiyar, V., Athimoolam, S., & Kanmani Pappa, C. (2024). Enhancing healthcare data security using quantum cryptography for efficient and robust encryption. *Journal of Educational Sciences*, 52(4), 44. **https://doi.org/10.52783/jes.2544**

Barbaria, S., Jemai, A., Ceylan, H. I., Muntean, R., Dergaa, I., & Rahmouni, H. B. (2025). Advancing compliance with HIPAA and GDPR in healthcare: A *Blockchain*-based strategy for secure data exchange in clinical research involving private health information. *Healthcare*, 13(20), 2594. **https://doi.org/10.3390/healthcare13202594**

Frempong, D., Benson, C. H., Oyasiji, O., & Okesiji, A. (2024). *Blockchain*-enabled consent management in healthcare: A framework for enforcing privacy preferences and regulatory compliance. *International Journal of Medical Research and General Exploration*, 5(3), 1059-1068. **https://doi.org/10.54660/.ijmrge.2024.5.3.1059-1068**

Jayaweera, R., Agrawal, H., & Karie, N. M. (2025). Federated security for privacy preservation of healthcare data in edge-cloud environments. *Sensors*, 25(16), 5108. **https://doi.org/10.3390/s25165108**

Jurczuk, M., & Suprunowicz, M. (2024). Consent in data privacy: A general comparison of GDPR and HIPAA. *Prace Uniwersytetu Jagiellskiego*, 16(7). **https://doi.org/10.14746/ppuam.2024.16.07**

Kunal, S., Gandhi, P., Rathod, D., Amin, R., & Sharma, S. (2024). Securing patient data in the healthcare industry: A *Blockchain*-driven protocol with advanced

encryption. *Journal of Education and Health Promotion*, 13(1), 984_23. **https://doi.org/10.4103/jehp.jehp_984_23**

M, & Triplett, W. J. (2024). Cybersecurity vulnerabilities in healthcare: A threat to patient security. *Current Issues in Technology and Informatics*, 2(1), 333. **https://doi.org/10.53889/citj.v2i1.333**

Nasar, M., Yousif, Y. K., Al Batahari, M., Kausar, M. A., Al-Dmour, N. A., & Saeed, A. Q. (2025). *Blockchain* for enhanced data privacy in healthcare. In *Proceedings of the IEEE International Conference on Blockchain and Applications* (pp. 11258491). **https://doi.org/10.1109/ICBATS66542.2025.11258491**

Shah, W. F. (2023). Preserving privacy and security: A comparative study of health data regulations - GDPR vs. HIPAA. *International Journal of Research and Applied Science*, 11(8), 55551. **https://doi.org/10.22214/ijraset.2023.55551**

Shojaei, P., Vlahu-Gjorgievska, E., & Chow, Y. W. (2024). Security and privacy of technologies in health information systems: A systematic literature review. *Computers*, 13(2), 41. **https://doi.org/10.3390/computers13020041**

Ts, S. (2025). Privacy-preserving health data sharing using secure MPC. *International Journal of Innovative Research and*

Advanced Engineering, 12(11), 14. **https://doi.org/10.26562/ijirae.2025.v1211.14**

Wani, R. U. Z., & Can, O. (2025). FED-EHR: A privacy-preserving federated learning framework for decentralized healthcare analytics. *Electronics*, 14(16), 3261. **https://doi.org/10.3390/electronics14163261**

Yadav, N. (2025). *Cloud Security: Zero Trust Architecture Guide*. Medium. Dipublikasikan 30 Juni 2025. **https://medium.com/@nitinyadav745/cloud-security-zero-trust-architecture-guide-fc4a8afc02a8**

Zaman, A., & Abuuzzam, A. A. (2024). Cybersecurity lessons from the Vastaamo psychotherapy data breach for psychiatrists and other mental healthcare providers. *The Australian and New Zealand Journal of Psychiatry*, 58(10), 1291340. **https://doi.org/10.1177/10398562241291340**

BAB 6
KEAMANAN DATA PADA PEMBIAYAAN KESEHATAN

Praditya Dewi Arumsari, S.E., M.Si

6.1 Alur Sistem Klaim Kesehatan

Tahap pertama dimulai saat pasien datang ke fasilitas kesehatan. Proses registrasi terdiri dari verifikasi identitas, pengecekan kepesertaan, dan input data ke sistem. Namun pada tahap inilah fondasi keamanan dibangun atau justru diabaikan. Data yang dikumpulkan bukan sekadar nama dan alamat, tetapi juga nomor identitas, riwayat penyakit, diagnosis, hingga rincian tindakan medis. Informasi ini bersifat sangat sensitif. Ketika data dimasukkan ke dalam EMR atau SIMRS, sistem tersebut menjadi "penjaga" pertama kerahasiaan pasien. Berbagai penelitian

menunjukkan bahwa banyak pelanggaran data justru terjadi akibat lemahnya kontrol akses, penggunaan kata sandi yang tidak memadai, atau kurangnya kesadaran keamanan di kalangan petugas (Hoffman, 2020). Serangan *phishing* terhadap petugas pendaftaran atau penyalahgunaan akses oleh orang dalam sering kali menjadi titik awal kebocoran data.

Tahap berikutnya adalah penyusunan dan pengiriman klaim. Pada fase ini, unit klaim menyusun dokumen berdasarkan standar pembiayaan yang berlaku, seperti INA-CBGs. Klaim tersebut dikirim secara elektronik ke pihak pembayar. Di sinilah data klinis bertemu dengan data finansial. Identitas pasien, diagnosis, tindakan medis, dan nilai klaim dikirimkan melalui jaringan digital. Tanpa enkripsi yang memadai, transmisi ini dapat menjadi celah bagi serangan *man-in-the-middle*, di mana pihak tidak berwenang dapat menyadap atau bahkan memodifikasi data klaim (Rahaman & Kudapa, 2022). Risiko ini menyebabkan perubahan kecil pada nilai klaim dapat berdampak signifikan terhadap keuangan sistem jaminan kesehatan. *Clearinghouse*, sebagai perantara administratif, memiliki peran penting dalam memastikan kelengkapan dan validitas klaim sebelum diteruskan kepada pihak pembayar. Ketika data dalam jumlah besar terkonsentrasi pada satu titik, risiko pelanggaran meningkat secara eksponensial. Studi mengenai keamanan sistem informasi kesehatan menunjukkan bahwa entitas agregator data memiliki potensi kerentanan yang lebih tinggi karena

menjadi target bernilai besar bagi pelaku kejahatan siber (Hatzivasilis et al., 2019).

Setelah melewati tahap verifikasi administratif, klaim masuk ke proses *review* oleh pihak asuransi atau BPJS. Pada tahap ini dilakukan verifikasi medis, audit pengkodean, serta deteksi potensi fraud. Sistem pembayar mengelola data dalam skala yang sangat besar, termasuk riwayat penyakit dan klaim sebelumnya. Ketika infrastruktur keamanan tidak dirancang dengan pendekatan berlapis, risiko serangan *ransomware* atau penyalahgunaan akses internal meningkat.

Tahap terakhir adalah settlement atau pembayaran. Pada fase ini, dana ditransfer ke rekening fasilitas kesehatan dan dilakukan rekonsiliasi. Meskipun tampak sebagai proses finansial rutin, risiko tetap ada. Business Email Compromise dan manipulasi nomor rekening menjadi modus kejahatan yang semakin sering terjadi dalam ekosistem pembayaran digital. Ketika keamanan tidak dijaga secara menyeluruh, dampaknya bukan hanya kebocoran data, tetapi juga kerugian finansial langsung.

6.2 Titik Rawan Kebocoran Data

Terdapat empat kategori utama kerentanan dalam sistem klaim kesehatan. Pertama adalah kebocoran identitas pasien. Data kesehatan memiliki nilai ekonomi tinggi karena tidak dapat dengan mudah diubah seperti nomor kartu kredit. *Medical identity theft* memungkinkan pelaku melakukan klaim palsu atau memperoleh

layanan atas nama korban. Dampaknya tidak hanya finansial, tetapi juga psikologis dan sosial, termasuk potensi diskriminasi berbasis kondisi medis (McCoy & Perlis, 2018). Kedua adalah penyadapan data selama transmisi klaim. Tanpa enkripsi *end-to-end*, data dapat diintersepsi dan dimodifikasi. Manipulasi kode diagnosis atau tarif layanan dapat menciptakan *fraud* yang sulit dideteksi. Oleh karena itu, pendekatan keamanan berbasis kecerdasan buatan dan deteksi anomali menjadi semakin relevan (Deep et al., 2024).

Ketiga adalah penyalahgunaan rekam medis untuk kepentingan *fraud*. Praktik seperti *upcoding* atau *phantom billing* bukan hanya pelanggaran etika, tetapi juga ancaman terhadap keberlanjutan sistem pembiayaan kesehatan. *Fraud* semacam ini menyebabkan pemborosan anggaran dan distorsi data epidemiologi yang digunakan dalam perencanaan kesehatan (Azad & William, 2024). Keempat adalah serangan siber terstruktur. Ketika sistem klaim lumpuh, pelayanan kesehatan dapat terganggu secara luas. Serangan semacam ini tidak hanya mengincar data, tetapi juga memanfaatkan ketergantungan sistem kesehatan terhadap teknologi digital.

6.3 Refleksi dan Implikasi

Pada akhirnya, sistem klaim kesehatan bukan sekadar prosedur administratif untuk menagihkan biaya pelayanan. Ia merupakan simpul penting dalam tata kelola sistem kesehatan nasional. Di dalamnya terdapat pertukaran data medis dan finansial yang bernilai tinggi dan sensitif. Semakin terdigitalisasi sistem

klaim, semakin besar pula kebutuhan akan arsitektur keamanan berbasis *zero trust*, integrasi kecerdasan buatan untuk deteksi *fraud*, serta peningkatan literasi keamanan siber bagi seluruh tenaga kesehatan dan administrator. Keamanan data bukan hanya tanggung jawab bagian IT, melainkan tanggung jawab kolektif seluruh aktor dalam sistem kesehatan.

DAFTAR PUSTAKA

Azad, T., & William, P. (2024). Fraud detection in healthcare billing and claims using machine learning approaches. *Journal of Healthcare Informatics Research.*

Deep, S., Kumar, S., & Kalra, P. (2024). AI-driven data security in healthcare: Safeguarding medical and financial transactions. *IEEE Access.*

Hatzivasilis, G., et al. (2019). Cyber insurance of information systems: Security and privacy cyber insurance contracts for ICT and healthcare organizations. *IEEE CAMAD.* https://doi.org/10.1109/CAMAD.2019.8858165

Hoffman, S. A. E. (2020). Cybersecurity threats in healthcare organizations: Exposing vulnerabilities in the healthcare information infrastructure. *World Libraries, 23*(1).

McCoy, T. H., & Perlis, R. H. (2018). Temporal trends and characteristics of reportable health data breaches, 2010–2017. *JAMA, 320*(12), 1282–1284. https://doi.org/10.1001/jama.2018.9222

Rahaman, M. M., & Kudapa, S. P. (2022). Information security challenges in healthcare payment ecosystems. *International Journal of Business and Economic Insights.*

BAB 7
PENGELOLAAN AKSES, PRIVASI, DAN HAK PASIEN

Dyah Ayu Puspitaningtyas,M.Tr.ID.

7.1 Konsep Akses Data Kesehatan dan Kerangka Hukum

7.1.1 Definisi Akses Data Kesehatan dan Hak Pasien

Akses data kesehatan mengacu pada kemampuan individu, institusi, atau pihak yang berwenang untuk memperoleh, melihat, atau menggunakan informasi kesehatan pasien yang tersimpan dalam berbagai sistem. Dalam konteks hak pasien, akses data kesehatan merupakan hak fundamental yang memberikan pasien kontrol atas informasi medis mereka sendiri, memastikan transparansi dalam penggunaan data, dan mendukung pengambilan keputusan yang diinformasikan tentang kesehatan mereka (Narkhede et al., 2025). Hak pasien untuk mengakses rekam medis mereka bukan hanya tentang akses fisik terhadap informasi, tetapi juga mencakup hak untuk memahami, mengoreksi, dan mengontrol penggunaan data tersebut. Sistem kesehatan modern harus menjamin bahwa pasien memiliki akses yang mudah, aman, dan transparan terhadap rekam medis elektronik (*electronic health records* atau EHR) mereka, sambil melindungi privasi dan keamanan data mereka dari akses yang tidak sah.

7.1.2 Kerangka Regulasi dan Standar Internasional

Kerangka regulasi untuk perlindungan akses dan privasi data kesehatan di tingkat global mencakup beberapa standar dan peraturan utama. Peraturan Perlindungan Data Umum atau *General Data Protection Regulation* (GDPR) di Eropa merupakan salah satu kerangka paling ketat yang memberikan individu kontrol penuh atas data pribadi mereka, termasuk hak untuk mengakses, memperbaiki, dan menghapus data (Nastasa et al., 2025). Di Amerika Serikat, *Health Insurance Portability and Accountability Act* (HIPAA) menetapkan standar untuk privasi dan keamanan informasi kesehatan yang dilindungi (*protected health information* atau PHI). Standar-standar internasional ini menekankan pentingnya informed consent, transparansi, dan keamanan data dalam pengelolaan informasi kesehatan pasien. Negara-negara berkembang seperti Indonesia juga telah mengadopsi kerangka regulasi serupa, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang memberikan kontrol lebih besar kepada pasien atas data kesehatan mereka (Pujihastuti et al., 2025).

7.1.3 Prinsip-Prinsip Dasar Pengelolaan Akses Data

Prinsip-prinsip dasar pengelolaan akses data kesehatan meliputi keamanan (*security*), kerahasiaan (*confidentiality*), integritas data (*data integrity*), ketersediaan (*availability*), dan

akuntabilitas. Keamanan data harus dimulai sejak data dikumpulkan hingga disimpan dan diakses, dengan implementasi enkripsi, autentikasi multi-faktor, dan sistem backup yang kuat. Kerahasiaan memastikan bahwa hanya individu yang berwenang yang dapat mengakses informasi kesehatan pasien. Integritas data menjamin bahwa informasi tidak diubah tanpa otorisasi, sedangkan ketersediaan memastikan bahwa data dapat diakses oleh pihak yang berwenang kapan diperlukan (Mulukutla, 2025). Akuntabilitas menciptakan jejak audit (*audit trail*) yang jelas untuk setiap akses dan perubahan data, memungkinkan organisasi kesehatan untuk melacak siapa yang mengakses data, kapan, dan untuk tujuan apa.

7.1.4 Peran Organisasi Kesehatan dalam Pengelolaan Akses

Organisasi kesehatan bertanggung jawab untuk mengimplementasikan kebijakan dan prosedur yang ketat dalam pengelolaan akses data kesehatan pasien. Tanggung jawab ini mencakup pembentukan komite etika dan kebijakan data, pelatihan staf tentang privasi dan keamanan data, implementasi sistem kontrol akses berbasis peran (*role-based access control* atau RBAC), dan monitoring berkelanjutan terhadap pengaksesan data (Olorunfemi et al., 2024). Organisasi kesehatan harus memastikan bahwa hanya staf yang memiliki kebutuhan bisnis yang sah (*need-to-know basis*) yang dapat mengakses data pasien, dan bahwa akses ini dicatat dan diaudit secara teratur. Organisasi juga harus memiliki kebijakan respons cepat terhadap pelanggaran data dan mekanisme pelaporan insiden

yang transparan untuk membangun kepercayaan pasien terhadap sistem kesehatan.

7.2 Privasi dan Keamanan Data Kesehatan

7.2.1 Strategi Perlindungan Privasi Data

Perlindungan privasi data kesehatan memerlukan pendekatan multi-lapis yang mengintegrasikan teknologi, kebijakan, dan praktik organisasi. Teknologi enkripsi merupakan salah satu pertahanan utama, dengan enkripsi data dalam transit menggunakan protokol seperti TLS (*Transport Layer Security*) dan enkripsi data dalam penyimpanan menggunakan algoritma seperti AES-256 (*Advanced Encryption Standard*) (Prasanna, 2025). Teknik anonimasi data seperti *de-identification*, *k-anonymity*, dan *differential privacy* dapat digunakan untuk melindungi privasi pasien dalam penelitian dan analisis data tanpa mengorbankan kegunaannya. Implementasi *privacy by design* memastikan bahwa perlindungan privasi dipertimbangkan sejak tahap desain sistem, bukan ditambahkan kemudian sebagai afterthought.

7.2.2 Teknologi *Blockchain* dan *Distributed Ledger*

Teknologi *Blockchain* menawarkan solusi inovatif untuk meningkatkan keamanan dan privasi data kesehatan dengan memberikan pasien kontrol lebih besar atas data mereka. *Blockchain* menciptakan ledger terdesentralisasi dan tidak dapat diubah yang mencatat setiap transaksi akses data, memastikan transparansi dan akuntabilitas (Tawfik et al., 2025). Sistem berbasis *Blockchain* dapat menggunakan *smart contracts* untuk mengotomatisasi proses

persetujuan akses (*consent*) dan membatasi akses berdasarkan keinginan pasien. Penelitian menunjukkan bahwa implementasi *Blockchain* dapat meningkatkan throughput hingga 19,7% dan mengurangi latency hingga 87% dibandingkan dengan sistem tradisional (Utami et al., 2025). Kombinasi *Blockchain* dengan enkripsi homomorphic memungkinkan analisis data yang dilakukan pada data terenkripsi tanpa perlu mendekripsi terlebih dahulu, meningkatkan privasi pasien selama proses penelitian.

7.2.3 Kontrol Akses Berbasis Atribut dan Role-Based Access Control

Sistem kontrol akses berbasis atribut (*Attribute-Based Access Control* atau ABAC) dan kontrol akses berbasis peran (*Role-Based Access Control* atau RBAC) memberikan cara yang granular untuk mengelola siapa yang dapat mengakses data kesehatan spesifik. RBAC membatasi akses berdasarkan peran pengguna dalam organisasi, misalnya dokter, perawat, atau administrator. ABAC lebih fleksibel, memungkinkan akses didasarkan pada kombinasi atribut seperti departemen pengguna, jenis data, waktu akses, dan lokasi (Turkstani et al., 2025). Implementasi *smart contracts* pada *Blockchain* dapat mengotomatisasi enforcement dari aturan akses ini dan memberikan audit trail yang tidak dapat diubah. Penelitian menunjukkan bahwa kombinasi enkripsi AES dan RSA dengan ABAC dapat mengurangi penggunaan penyimpanan sebesar 27% dan meningkatkan kecepatan retrieval data sebesar 35%.

7.2.4 Deteksi dan Respons Terhadap Pelanggaran Data

Sistem deteksi pelanggaran data menggunakan teknik seperti *anomaly detection* berbasis *machine learning* dapat mengidentifikasi akses yang tidak biasa atau mencurigakan terhadap data kesehatan pasien (V et al., 2025). Organisasi kesehatan harus memiliki kebijakan respons insiden yang jelas dan terlatih, termasuk prosedur untuk mengisolasi sistem yang terpengaruh, melakukan investigasi root-cause analysis, dan memberitahu pasien yang data-nya terpengaruh sesuai dengan persyaratan regulasi. Laporan pelanggaran data harus dikomunikasikan kepada regulator dan pihak yang terkena dampak dalam jangka waktu yang ditentukan, biasanya dalam hitungan hari. Organisasi kesehatan juga harus mempertahankan asuransi cyber dan memiliki rencana continuity bisnis untuk memastikan layanan kesehatan dapat terus beroperasi meskipun terjadi pelanggaran data.

7.3 Informed Consent dan Otonomi Pasien

7.3.1 Konsep Informed Consent dalam Konteks Digital

Informed consent atau persetujuan berdasarkan informasi merupakan prinsip etis fundamental yang mengharuskan pasien memberikan persetujuan secara sukarela berdasarkan pemahaman penuh tentang risiko dan manfaat dari suatu tindakan medis atau penggunaan data mereka. Dalam konteks digital, informed consent menghadapi tantangan baru karena kompleksitas teknologi, multiple stakeholders dalam ekosistem data kesehatan digital, dan kesulitan pasien memahami implikasi penuh dari penggunaan data

mereka (Amin et al., 2024). Informed consent yang efektif dalam setting digital memerlukan komunikasi yang jelas tentang bagaimana data akan digunakan, siapa yang akan mengakses data, berapa lama data akan disimpan, dan hak pasien untuk membatasi atau mencabut consent mereka. Platform digital harus menyediakan informasi dalam bahasa yang mudah dipahami, bukan jargon teknis atau hukum yang kompleks.

7.3.2 Model Consent Dinamis dan Granular

Model consent tradisional yang memberikan satu-kali persetujuan untuk semua penggunaan data tidak lagi sesuai untuk konteks digital yang kompleks dan dinamis. Model *dynamic consent* dan *granular consent* memungkinkan pasien untuk memberikan persetujuan yang spesifik untuk berbagai jenis penggunaan data, memperbaharui consent mereka kapan saja, dan menarik consent untuk penggunaan data tertentu (Narkhede et al., 2025). Sistem consent granular memungkinkan pasien memilih data mana yang ingin dibagikan, dengan siapa, dan untuk tujuan apa. Implementasi smart contracts berbasis *Blockchain* dapat mengotomatisasi enforcement dari preferensi consent pasien dan menciptakan audit trail yang transparan dari semua akses data. Platform seperti Australia's My Health Record mendemonstrasikan potensi patient-centric consent frameworks dalam meningkatkan kepercayaan pasien terhadap sistem kesehatan digital.

7.3.3 Tantangan Informed Consent untuk Penggunaan Sekunder Data

Penggunaan sekunder data kesehatan, yaitu penggunaan data yang dikumpulkan awalnya untuk tujuan klinis untuk penelitian dan analisis, menghadirkan tantangan etis dan praktis dalam memperoleh informed consent yang bermakna. Pasien mungkin kesulitan memahami semua kemungkinan penggunaan penelitian di masa depan dari data mereka, sehingga model broad consent atau opt-out consent sering digunakan di tempat konsens spesifik (Mann et al., 2016). Namun, beberapa organisasi kesehatan menggunakan consent exemptions untuk penelitian yang melibatkan minimal risk, berdasarkan prinsip *duty of easy rescue* yang menyatakan bahwa individu harus membantu orang lain ketika dapat melakukannya tanpa risiko signifikan terhadap diri mereka sendiri. Penelitian menunjukkan bahwa interaksi tatap muka saat memperoleh informed consent menghasilkan tingkat consent yang lebih tinggi dibandingkan dengan pendekatan telepon atau email, terutama pada populasi yang rentan.

7.3.4 Hak Otonomi Pasien dan Right to be Forgotten

Otonomi pasien dalam konteks data kesehatan digital mencakup hak untuk membuat keputusan tentang kesehatan mereka berdasarkan informasi lengkap, hak untuk mengakses data mereka, dan hak untuk membatasi atau menghapus data mereka. Right to be forgotten (*right to erasure*), yang diakui dalam GDPR, memberikan pasien hak untuk menghapus data pribadi mereka dalam kondisi tertentu (Mohile, 2025). Namun, dalam konteks kesehatan, right to be forgotten dapat menimbulkan dilema karena informasi medis

mungkin penting untuk perawatan pasien di masa depan atau untuk tujuan kesehatan masyarakat. Organisasi kesehatan harus memiliki kebijakan yang jelas tentang bagaimana mereka menangani permintaan penghapusan data sambil mempertahankan catatan medis yang lengkap dan akurat untuk kepentingan pasien dan publik. Right to not know tentang informasi genetik tertentu juga perlu dipertimbangkan dalam era genomics, memungkinkan pasien untuk memilih tidak mengetahui informasi yang dapat menyebabkan distres psikologis atau diskriminasi.

7.4 Kebijakan dan Manajemen Akses dalam Praktik

7.4.1 Kebijakan Akses Berbasis Kebutuhan Bisnis dan Least Privilege Principle

Kebijakan akses data kesehatan harus didasarkan pada prinsip *least privilege*, yang menyatakan bahwa setiap pengguna harus diberikan akses minimum yang diperlukan untuk melakukan pekerjaan mereka. Penerapan prinsip ini memerlukan identifikasi yang jelas tentang tugas-tugas yang berbeda dalam organisasi kesehatan dan data yang diperlukan untuk setiap tugas. Audit akses berkala harus dilakukan untuk memastikan bahwa pengguna masih memiliki kebutuhan bisnis yang sah untuk akses yang mereka terima, dan akses yang tidak lagi diperlukan harus segera dicabut (Rinchen & Yoezer, 2024). Dokumentasi kebijakan akses harus transparan, dapat diakses oleh karyawan, dan diperbarui secara berkala untuk mencerminkan perubahan dalam operasi organisasi.

7.4.2 Training dan Kesadaran Karyawan tentang Privasi dan Keamanan

Pelatihan karyawan merupakan komponen kritis dalam pengelolaan akses data kesehatan yang efektif, karena sebagian besar pelanggaran data disebabkan oleh kesalahan manusia atau perilaku yang tidak sesuai dengan kebijakan. Program pelatihan harus mencakup topik seperti pentingnya kerahasiaan pasien, cara mengidentifikasi serangan phishing dan social engineering, prosedur reporting inciden, dan konsekuensi dari pelanggaran kebijakan privasi (Alhomidan et al., 2025). Pelatihan harus diberikan kepada semua karyawan, bukan hanya staf teknis, karena semua orang yang bekerja dengan data kesehatan pasien memiliki tanggung jawab untuk menjaganya. Pelatihan harus dilakukan secara berkala, dengan konten yang diperbarui untuk mencerminkan ancaman keamanan terbaru dan perubahan dalam kebijakan organisasi.

7.4.3 Audit dan Monitoring Berkelanjutan Terhadap Akses Data

Audit dan monitoring terhadap akses data kesehatan memastikan bahwa hanya pengguna yang berwenang mengakses data, dan bahwa akses ini dilakukan sesuai dengan kebijakan organisasi. Sistem audit harus menciptakan log yang detail tentang siapa yang mengakses data, kapan, apa yang mereka lihat atau ubah, dan untuk tujuan apa (Jayakumar et al., 2024). Analisis log ini dapat mengidentifikasi pola akses yang mencurigakan, seperti akses

malam hari, akses dari lokasi yang tidak biasa, atau akses data dalam volume yang abnormal. Alert real-time dapat ditetapkan untuk memberitahu administrator tentang aktivitas yang mencurigakan. Audit internal harus dilakukan secara regular untuk memastikan kepatuhan terhadap kebijakan, dan hasil audit harus dikomunikasikan kepada manajemen dan dewan organisasi.

7.4.4 Mekanisme Pengaduan dan Resolusi Pelanggaran Privasi

Organisasi kesehatan harus memiliki mekanisme yang mudah diakses dan responsif bagi pasien untuk melaporkan kekhawatiran tentang privasi data mereka atau pelanggaran yang dicurigai. Mekanisme pengaduan harus independen dari struktur manajemen normal, sehingga pasien merasa aman melaporkan masalah tanpa takut perlakuan balas (Ibrahim et al., 2024). Proses investigasi harus dilakukan secara profesional dan cepat, dengan komunikasi yang jelas kepada pasien tentang temuan dan tindakan yang diambil. Organisasi harus memiliki kebijakan untuk memberikan notifikasi kepada pasien jika privasi mereka terganggu, dan harus menawarkan layanan monitoring kredit atau dukungan psikologis jika diperlukan. Hasil investigasi harus didokumentasikan dengan baik dan digunakan untuk melakukan perbaikan sistem guna mencegah insiden serupa di masa depan.

7.5 Tantangan dan Solusi Inovatif dalam Pengelolaan Akses dan Privasi

7.5.1 Tantangan Keseimbangan Antara Privasi dan Inovasi Kesehatan

Salah satu tantangan utama dalam pengelolaan akses dan privasi data kesehatan adalah keseimbangan antara perlindungan privasi pasien dan fasilitasi inovasi dalam penelitian biomedis dan pengembangan terapi baru. Pembatasan akses yang terlalu ketat terhadap data kesehatan dapat menghambat penelitian penting yang dapat menguntungkan masyarakat luas, sementara akses yang terlalu longgar dapat membahayakan privasi pasien individual. Solusi inovatif seperti federated learning memungkinkan tim peneliti di berbagai institusi untuk mengembangkan model machine learning pada data terdesentralisasi tanpa memerlukan akses langsung ke data pasien individual (E et al., 2025). Teknik differential privacy dapat diterapkan untuk memastikan bahwa hasil analisis tidak mengungkapkan informasi tentang individu tertentu. Privacy-preserving analytics framework memungkinkan organisasi kesehatan untuk melakukan analisis data yang bermakna sambil mempertahankan kerahasiaan pasien.

7.5.2 Interoperabilitas dan Pertukaran Data Lintas Institusi

Tantangan signifikan dalam pengelolaan akses dan privasi adalah memfasilitasi pertukaran data kesehatan lintas institusi sambil mempertahankan keamanan dan privasi. Pasien seringkali menerima perawatan dari berbagai penyedia kesehatan yang

menggunakan sistem EHR yang berbeda-beda dan tidak terintegrasi. Kemampuan untuk berbagi data secara aman lintas institusi penting untuk kontinuitas perawatan dan penelitian kolaboratif, namun menciptakan risiko keamanan yang kompleks. Solusi seperti FHIR (*Fast Healthcare Interoperability Resources*) standards dan *Blockchain*-based health information exchange dapat memfasilitasi pertukaran data yang aman dan interoperable (Okemwa et al., 2025). Sistem ini menggunakan identifikasi yang terenkripsi dan access control berbasis atribut untuk memastikan bahwa data hanya dibagikan kepada penyedia yang memiliki kebutuhan bisnis yang sah dan dengan persetujuan pasien.

7.5.3 Privasi dalam Era Artificial Intelligence dan Genomics

Adopsi kecepatan AI dan teknologi genomics dalam kesehatan menciptakan tantangan privasi baru. Model AI dapat mengungkapkan pola tersembunyi dalam data kesehatan yang dapat mengidentifikasi kembali pasien individual dari data yang seharusnya anonim. Informasi genetik sensitif yang terintegrasi dengan EHR menciptakan risiko diskriminasi genetik dari asuransi atau penyedia. Solusi mencakup implementasi model AI yang interpretable dan explainable, penggunaan synthetic data untuk pengembangan model, dan governance frameworks yang jelas untuk penggunaan data genetik (Joshi et al., 2025). Ethical oversight dari research involving genomic data harus diperkuat, dengan pertimbangan khusus terhadap kemungkinan incidental findings dan implikasi untuk keluarga pasien yang berbagi informasi genetik.

7.5.4 Kesadaran Pasien dan Literasi Digital

Banyak pasien tidak memahami sepenuhnya bagaimana data kesehatan mereka digunakan, bagaimana teknologi melindungi privasi mereka, dan hak-hak apa yang mereka miliki terkait data mereka. Kurangnya literasi digital membuat pasien rentan terhadap eksploitasi data dan membuat mereka tidak dapat memberikan informed consent yang bermakna. Program pendidikan pasien harus dikembangkan untuk meningkatkan kesadaran tentang pentingnya privasi data, risiko keamanan cyber, dan cara pasien dapat melindungi data mereka (Ahmad et al., 2024). Media sosial dan platform patient engagement dapat digunakan untuk menyebarkan informasi tentang privasi dan keamanan data secara accessible dan engaging. Organisasi kesehatan harus menyediakan layanan dukungan untuk membantu pasien memahami dan mengelola preferensi privasi mereka dalam sistem EHR.

Latihan Soal

1. Jelaskan bagaimana prinsip *least privilege* dan *role-based access control* dapat diterapkan dalam sistem EHR untuk memastikan bahwa data kesehatan pasien hanya diakses oleh personel yang memiliki kebutuhan bisnis yang sah. Apa tantangan dalam implementasi prinsip ini di rumah sakit yang kompleks?
2. Analisis perbedaan antara model *informed consent* tradisional dengan *dynamic consent* dan *granular consent*. Bagaimana smart contracts berbasis *Blockchain* dapat meningkatkan efektivitas pengelolaan consent dalam konteks digital?
3. Diskusikan dilema etis antara perlindungan privasi pasien dan fasilitasi penelitian biomedis yang dapat menguntungkan masyarakat luas. Jelaskan bagaimana teknik seperti federated learning dan differential privacy dapat membantu mengatasi dilema ini.
4. Evaluasi potensi dan tantangan dalam mengadopsi teknologi *Blockchain* untuk pengelolaan akses dan privasi data kesehatan. Apa kelebihan *Blockchain* dibandingkan dengan sistem terpusat tradisional, dan apa hambatan implementasinya?
5. Jelaskan bagaimana organisasi kesehatan dapat mengelola keseimbangan antara akses data yang diperlukan untuk perawatan pasien yang optimal dan pembatasan akses untuk melindungi privasi pasien. Apa peran audit dan monitoring berkelanjutan dalam mencapai keseimbangan ini?

DAFTAR PUSTAKA

Narkhede, M., Wankhede, N. I., & Kamble, A. M. (2025). Enhancing patient autonomy in data ownership: Privacy models and consent frameworks for healthcare. *Journal of Digital Health*, 4(2), 513361-23. **https://doi.org/10.55976/jdh.4202513361-23**

Pujihastuti, A., Manggandhi, Y., & Rafika, K. (2025). The impact of the latest health data privacy regulations on patient information access policies in healthcare service facilities. *Jurnal Rekam Medis*, 1(2), 306. **https://doi.org/10.69855/rekammedis.v1i2.306**

Mohile, K. (2025). Navigating the balance: Ethics at the crossroads of healthcare data security and patient privacy. *World Journal of Advanced Research and Reviews*, 26(2), 1622. **https://doi.org/10.30574/wjarr.2025.26.2.1622**

Prasanna, G. L. (2025). Privacy preserving data sharing cloud-based healthcare systems. *International Journal of Scientific Research and Engineering Management*, 40474. **https://doi.org/10.55041/ijsrem40474**

Tawfik, A. M., Al-ahwal, A., Tag Eldien, A. S., & Zayed, H. (2025). ACHealthChain *Blockchain* framework for access control and privacy preservation in healthcare. *Scientific Reports*, 25, 00757-1. **https://doi.org/10.1038/s41598-025-00757-1**

Sivanantham E., Raghavendra C., Faisal M., Poovizhi S., Sujatha S., & Palanivel V. (2025). Privacy-preserving patient consent

management using federated learning and cloud technology in digital health. *IEEE International Conference on Communications, Signal Processing and their Applications*, 11089319. **https://doi.org/10.1109/ICCSP64183.2025.11089319**

Mulukutla, K. (2025). Ensuring data privacy and compliance in healthcare analytics. *International Journal of Cultural and Social Studies*, 4176. **https://doi.org/10.22399/ijcesen.4176**

Turkstani, H. A., Almutawah, F. N., AlZamel, N. A., Alshammari, M. Z., Alhamadi, A. A., Algharbi, M. T., Alsuayri, A. M., Gong, M. B., Alqahtani, J., Alnemer, A. F., & Aljuwayed, N. H. (2025). Privacy and confidentiality in healthcare: Best practices for protecting patient information. *Journal of Healthcare Sciences*, 50(1), 06. **https://doi.org/10.52533/johs.2025.50106**

Chakravarthy, D. G., Gopi, R., Murugan, S., & Joseph, E. R. (2025). Enhancing confidentiality and access control in electronic health record systems using a hybrid hashing *Blockchain* framework. *Scientific Reports*, 25, 13831-5. **https://doi.org/10.1038/s41598-025-13831-5**

Olorunfemi, O., Oyegoke, E. O., Abiodun, O. O., Kunle-Abioye, F. B., & Ayeni, B. A. (2024). Achieving a balance between ethical and legal obligations with regard to confidentiality and patient privacy. *American Journal of Medical Sciences*, 2024(1), 7-24. **https://doi.org/10.4103/amjm.amjm_7_24**

BAB 8
AUDIT, PENGAWASAN, DAN KEPATUHAN PERLINDUNGAN DATA

Rudiansyah, SKM., M. Kes

8.1 Prinsip-Prinsip Dasar Audit dan Pengawasan Perlindungan Data

8.1.1 Definisi dan Tujuan Audit Perlindungan Data

Audit perlindungan data merupakan evaluasi sistematis dan independen terhadap kepatuhan organisasi terhadap peraturan perlindungan data dan keamanan informasi yang berlaku. *Data protection audit* adalah proses untuk menilai bagaimana organisasi mengumpulkan, memproses, menyimpan, dan melindungi data pribadi dari akses tidak sah, kehilangan, atau penyalahgunaan. Tujuan utama audit perlindungan data adalah memastikan bahwa organisasi telah mengimplementasikan kontrol teknis dan organisasi yang memadai, mengidentifikasi celah dalam kepatuhan, dan memberikan rekomendasi untuk perbaikan (Nangi & Obannagari, 2025).

Audit perlindungan data juga berfungsi untuk membangun kepercayaan dengan pemangku kepentingan, termasuk pelanggan, regulator, dan mitra bisnis. Dengan melakukan audit secara berkala,

organisasi dapat menunjukkan komitmen mereka terhadap perlindungan data dan meminimalkan risiko terhadap pelanggaran dan sanksi regulasi. Audit yang efektif harus mencakup evaluasi terhadap kebijakan, proses, teknologi, dan sumber daya manusia yang terlibat dalam penanganan data (Goyal et al., 2025).

8.1.2 Kerangka Kerja Audit dan Standar Internasional

Terdapat beberapa kerangka kerja dan standar internasional yang dapat digunakan sebagai panduan dalam melakukan audit perlindungan data. Standar ISO 27001 menyediakan kerangka kerja komprehensif untuk manajemen keamanan informasi, termasuk kontrol yang relevan dengan perlindungan data. GDPR (General Data Protection Regulation) di Eropa dan HIPAA (Health Insurance Portability and Accountability Act) di Amerika Serikat memberikan persyaratan audit dan dokumentasi yang spesifik. Organisasi harus memilih kerangka kerja yang sesuai dengan konteks bisnis dan persyaratan regulasi yang berlaku (Raveendran, 2025).

Kerangka kerja audit yang baik harus mencakup: (1) Ruang lingkup audit yang jelas dan komprehensif; (2) Kriteria audit yang didefinisikan dengan baik berdasarkan standar internasional dan regulasi lokal; (3) Metodologi audit yang terstruktur dan konsisten; (4) Proses pelaporan yang transparan; dan (5) Mekanisme tindak lanjut untuk mengatasi temuan audit (Bakare et al., 2024). Dengan menggunakan kerangka kerja yang terstandar, organisasi dapat memastikan bahwa audit mereka konsisten, dapat dibandingkan, dan selaras dengan ekspektasi regulasi.

8.1.3 Peran Auditor dan Kompetensi yang Diperlukan

Auditor perlindungan data memiliki peran penting dalam memastikan kepatuhan organisasi terhadap regulasi perlindungan data. Auditor harus memiliki pemahaman mendalam tentang peraturan perlindungan data yang berlaku, termasuk GDPR, HIPAA, CCPA, dan regulasi lokal lainnya. Selain itu, auditor harus memiliki keahlian teknis dalam keamanan informasi, manajemen risiko, dan pengelolaan data. Kompetensi penting bagi auditor termasuk kemampuan untuk melakukan penilaian risiko, menganalisis teknik enkripsi dan akses kontrol, serta memahami proses bisnis organisasi (Rachapalli, 2022).

Auditor yang independen dan kompeten sangat penting untuk kredibilitas proses audit. Organisasi sebaiknya menggunakan kombinasi auditor internal yang memahami operasi mereka dan auditor eksternal yang memberikan perspektif independen. Pelatihan berkelanjutan bagi auditor juga sangat penting untuk memastikan mereka tetap mutakhir dengan perkembangan teknologi dan perubahan regulasi (Verma, 2025).

8.1.4 Siklus Audit dan Frekuensi Audit

Siklus audit perlindungan data harus dirancang untuk memastikan cakupan komprehensif dari semua aspek pengelolaan data dalam organisasi. *Audit cycle* yang efektif biasanya mengikuti pendekatan *plan-do-check-act* (PDCA), dimulai dengan perencanaan audit, pelaksanaan audit, analisis temuan, dan

implementasi tindakan perbaikan. Frekuensi audit harus ditentukan berdasarkan tingkat risiko, ukuran organisasi, dan peraturan yang berlaku. Organisasi dengan operasi yang kompleks dan menangani data sensitif biasanya memerlukan audit tahunan atau semi-tahunan (Bellala, 2025).

Perencanaan audit harus dimulai dengan identifikasi area-area berisiko tinggi yang memerlukan perhatian khusus, pengembangan rencana audit yang detail, dan alokasi sumber daya yang memadai. Selama pelaksanaan audit, auditor melakukan pengujian kontrol, wawancara dengan staf, dan pengumpulan bukti. Setelah audit selesai, temuan harus didokumentasikan dengan jelas dan rekomendasi harus dikembangkan untuk perbaikan. Organisasi harus melacak tindak lanjut terhadap rekomendasi audit dan memastikan implementasi yang tepat waktu (Garg, 2024).

8.2 Mekanisme Pengawasan Berkelanjutan Perlindungan Data

8.2.1 Monitoring dan *Compliance Tracking* Real-Time

Pengawasan berkelanjutan (*continuous monitoring*) adalah pendekatan modern untuk memastikan kepatuhan perlindungan data yang terus-menerus, bukan hanya pada saat audit periodik. *Real-time monitoring* menggunakan teknologi otomasi untuk melacak akses data, mengidentifikasi aktivitas mencurigakan, dan mendeteksi potensi pelanggaran keamanan secara real-time. Sistem monitoring yang baik harus mencatat semua transaksi yang

melibatkan data pribadi, termasuk siapa yang mengakses, kapan, dari mana, dan untuk apa (Nangi & Obannagari, 2025).

Compliance tracking melibatkan pengumpulan dan analisis data tentang kinerja organisasi terhadap persyaratan perlindungan data. Metrik kunci yang harus dilacak mencakup: (1) Jumlah permintaan akses data yang diproses; (2) Waktu rata-rata untuk merespons permintaan subjek data; (3) Insiden keamanan yang terdeteksi; (4) Tingkat kepatuhan terhadap kebijakan perlindungan data; dan (5) Hasil pelatihan karyawan (Goyal et al., 2025). Dengan melacak metrik ini secara real-time, organisasi dapat dengan cepat mengidentifikasi masalah dan mengambil tindakan korektif.

8.2.2 Sistem Logging dan Audit Trail

Audit trail yang komprehensif merupakan fondasi dari pengawasan perlindungan data yang efektif. *Audit trail* adalah catatan terperinci dari semua aktivitas yang terkait dengan akses dan penggunaan data, disimpan dalam format yang tidak dapat diubah dan dapat diverifikasi. Sistem logging yang baik harus mencatat informasi seperti identitas pengguna, waktu akses, data yang diakses, tindakan yang dilakukan (misalnya, baca, tulis, hapus), hasil tindakan (sukses atau gagal), dan alamat IP pengguna (Rachapalli, 2022).

Untuk memastikan integritas audit trail, log harus disimpan di lokasi yang aman dan terlindungi dari akses tidak sah. Organisasi harus mengimplementasikan mekanisme untuk mencegah penghapusan atau modifikasi log yang tidak sah, seperti penggunaan

enkripsi, *write-once storage*, atau salinan offline. Log harus dipertahankan untuk periode waktu yang ditentukan oleh regulasi, biasanya minimal satu tahun, dan dianalisis secara berkala untuk mendeteksi pola aktivitas yang mencurigakan (Barbaria et al., 2025).

8.2.3 Deteksi Anomali dan Sistem Peringatan Dini

Sistem deteksi anomali menggunakan *machine learning* dan analitik data untuk mengidentifikasi pola aktivitas yang tidak normal atau mencurigakan dalam penggunaan data. Anomali dapat mencakup akses yang tidak biasa ke data sensitif, transfer data dalam jumlah besar, akses dari lokasi geografis yang tidak biasa, atau penggunaan privile tinggi yang tidak diharapkan. Dengan mendeteksi anomali secara otomatis, organisasi dapat merespons dengan cepat terhadap potensi pelanggaran keamanan (Avireneni, 2025).

Sistem peringatan dini (*early warning system*) memberitahu administrator atau tim keamanan ketika aktivitas mencurigakan terdeteksi, memungkinkan investigasi dan tindakan korektif yang cepat. Sistem ini harus dapat dikonfigurasi untuk menyesuaikan dengan profil risiko spesifik organisasi dan harus meminimalkan *false positives* yang dapat mengakibatkan *alert fatigue*. Integrasi dengan sistem *incident response* memastikan bahwa peringatan diikuti dengan tindakan yang tepat dan didokumentasikan dengan baik (Oladosu et al., 2021).

8.2.4 Pelaporan dan Transparansi Pengawasan

Pelaporan hasil pengawasan perlindungan data kepada stakeholder yang relevan adalah bagian penting dari kepatuhan. Laporan harus jelas, komprehensif, dan menunjukkan tingkat kepatuhan organisasi terhadap persyaratan perlindungan data. Laporan harus mencakup ringkasan metrik kepatuhan, temuan dari monitoring berkelanjutan, insiden keamanan yang terjadi, dan tindakan perbaikan yang telah atau akan diambil (Cadet et al., 2024).

Transparansi dalam pengawasan membangun kepercayaan dengan pemangku kepentingan dan menunjukkan bahwa organisasi mengambil perlindungan data dengan serius. Organisasi harus menyediakan laporan secara berkala kepada manajemen, dewan direksi, dan jika diperlukan, kepada otoritas pengawas. Laporan harus mencakup tidak hanya metrik kepatuhan tetapi juga analisis tren, identifikasi area risiko baru, dan rekomendasi untuk peningkatan berkelanjutan (Conduah et al., 2025).

8.3 Kepatuhan terhadap Regulasi Perlindungan Data Global

8.3.1 GDPR dan Persyaratan Kepatuhan di Eropa

General Data Protection Regulation (GDPR) merupakan regulasi perlindungan data paling komprehensif di dunia dan berlaku di Eropa serta memiliki dampak global untuk organisasi yang menangani data warga Eropa. GDPR menetapkan persyaratan ketat untuk pengumpulan, pemrosesan, dan penyimpanan data pribadi. Salah satu persyaratan penting adalah bahwa organisasi harus

melakukan *privacy impact assessment* (DPIA) sebelum melakukan pemrosesan data yang berisiko tinggi (Goyal et al., 2025).

GDPR mengharuskan organisasi untuk menunjukkan kepatuhan melalui *accountability* dan dokumentasi. Organisasi harus memiliki *Data Protection Officer* (DPO) yang bertanggung jawab untuk memastikan kepatuhan terhadap GDPR. DPO harus melakukan audit regular, menjawab permintaan dari otoritas perlindungan data, dan melaporkan pelanggaran data ke otoritas dan individu yang terkena dampak. Pelanggaran GDPR dapat mengakibatkan denda hingga 4% dari pendapatan tahunan global perusahaan atau 20 juta euro, mana yang lebih besar (Bakare et al., 2024).

8.3.2 HIPAA dan Kepatuhan Perlindungan Data Kesehatan

Health Insurance Portability and Accountability Act (HIPAA) adalah regulasi utama di Amerika Serikat yang mengatur perlindungan informasi kesehatan yang terlindungi (PHI). HIPAA memiliki tiga komponen utama: *Privacy Rule*, *Security Rule*, dan *Breach Notification Rule*. *Privacy Rule* mengatur bagaimana PHI dapat digunakan dan diungkapkan. *Security Rule* memerlukan implementasi perlindungan fisik, teknis, dan administratif untuk melindungi PHI. *Breach Notification Rule* mengharuskan organisasi untuk melaporkan pelanggaran keamanan data kepada individu yang terkena dampak dan otoritas (Raveendran, 2025).

Organisasi yang mematuhi HIPAA harus melakukan audit keamanan secara berkala, mengimplementasikan kontrol akses yang ketat, mempertahankan log audit yang komprehensif, dan memiliki rencana respons insiden yang jelas. Pelanggaran HIPAA dapat mengakibatkan denda signifikan dan kerusakan reputasi. Organisasi harus melakukan audit HIPAA secara periodik untuk memastikan bahwa semua persyaratan telah dipenuhi dan untuk mengidentifikasi area yang memerlukan perbaikan (Barbaria et al., 2025).

8.3.3 Regulasi Perlindungan Data Lokal dan Regional

Selain GDPR dan HIPAA, berbagai yurisdiksi telah mengembangkan peraturan perlindungan data mereka sendiri. California Consumer Privacy Act (CCPA) di Amerika Serikat memberikan konsumen hak untuk mengetahui data yang dikumpulkan tentang mereka, hak untuk menghapus data, dan hak untuk memilih keluar dari penjualan data. Organisasi yang melayani konsumen di California harus mematuhi CCPA dan melakukan audit untuk memastikan kepatuhan (Bellala, 2025).

Di negara lain, regulasi seperti Protection of Personal Information Act (POPIA) di Afrika Selatan, Personal Information Protection and Electronic Documents Act (PIPEDA) di Kanada, dan berbagai regulasi di negara Asia-Pasifik menetapkan persyaratan perlindungan data yang berbeda. Organisasi yang beroperasi secara global harus memahami persyaratan regulasi di setiap yurisdiksi di mana mereka beroperasi dan melakukan audit untuk memastikan kepatuhan (Idoko et al., 2024).

8.3.4 Harmonisasi dan Keselarasan Regulasi Internasional

Dengan banyaknya regulasi perlindungan data yang berbeda di seluruh dunia, organisasi global menghadapi tantangan dalam mencapai kepatuhan di berbagai yurisdiksi. Strategi yang efektif adalah mengadopsi standar perlindungan data yang paling ketat dan menerapkannya secara global, sambil memastikan kepatuhan dengan persyaratan lokal spesifik. Ini dikenal sebagai pendekatan *privacy by design and by default* (Goyal et al., 2025).

Organisasi juga dapat memanfaatkan keselarasan antara regulasi yang berbeda. Sebagai contoh, banyak aspek GDPR dan HIPAA memiliki prinsip yang sama, seperti kebutuhan untuk transparansi, kontrol akses, dan dokumentasi. Dengan mengimplementasikan kontrol yang memenuhi persyaratan GDPR, organisasi dapat dengan lebih mudah mencapai kepatuhan terhadap HIPAA dan regulasi lainnya. Bagaimanapun, organisasi harus tetap waspada terhadap perbedaan penting dan memastikan bahwa mereka tidak mengabaikan persyaratan spesifik dalam setiap regulasi (Garg, 2024).

8.4 Implementasi Teknologi untuk Audit dan Kepatuhan Otomatis

8.4.1 Otomasi Audit dan Sistem Berbasis Kecerdasan Buatan

Otomasi audit menggunakan teknologi seperti kecerdasan buatan (*artificial intelligence*) dan pembelajaran mesin (*machine learning*) untuk melakukan tugas-tugas audit yang berulang secara

otomatis dan efisien. Sistem berbasis AI dapat menganalisis volume besar data log, mengidentifikasi pola anomali, dan mengevaluasi kepatuhan terhadap kebijakan perlindungan data dengan kecepatan dan akurasi yang lebih tinggi daripada audit manual (Nangi & Obannagari, 2025).

AI-driven compliance monitoring dapat memberikan hasil yang lebih konsisten dan mengurangi kesalahan manusia. Sistem ini dapat secara real-time mengevaluasi setiap aktivitas terhadap kebijakan yang telah didefinisikan dan memberikan peringatan ketika terjadi penyimpangan. Sistem otomasi juga dapat membantu organisasi merespons audit reguler dengan cepat dengan menghasilkan laporan yang menunjukkan kepatuhan terhadap persyaratan spesifik (Goyal et al., 2025).

8.4.2 *Privacy-as-Code* dan *Compliance-as-Code*

Pendekatan *privacy-as-code* dan *compliance-as-code* mengubah kebijakan perlindungan data dan persyaratan kepatuhan menjadi kode yang dapat dijalankan secara otomatis. Dengan cara ini, kebijakan dapat diberlakukan secara konsisten di seluruh organisasi dan sistem dapat secara otomatis memverifikasi kepatuhan. Sebagai contoh, aturan akses kontrol dapat didefinisikan sebagai kode dan sistem dapat secara otomatis memeriksa bahwa pengguna tidak memiliki akses yang melebihi otorisasi mereka (Rachapalli, 2022).

Penggunaan *Infrastructure-as-Code* (IaC) dan *Policy-as-Code* memungkinkan organisasi untuk mendefinisikan, mengelola,

dan mengaudit kebijakan perlindungan data dengan cara yang terotomasi dan dapat dilacak. Setiap perubahan kebijakan dapat dicatat, diaudit, dan dikembalikan jika diperlukan. Pendekatan ini meningkatkan konsistensi, mengurangi risiko kesalahan manusia, dan membuat audit kepatuhan menjadi lebih efisien (Samala, 2025).

8.4.3 *Blockchain* dan Audit Trail Tidak Dapat Diubah

Blockchain dapat digunakan untuk menciptakan audit trail yang tidak dapat diubah dan transparan untuk semua aktivitas yang berkaitan dengan penanganan data. Dengan menggunakan *Blockchain*, setiap aktivitas dicatat dalam blok yang dikriptografi dan terhubung dengan blok sebelumnya, membuat tidak mungkin untuk mengubah atau menghapus catatan tanpa terdeteksi. Smart contracts dapat digunakan untuk secara otomatis memberlakukan kebijakan akses dan kepatuhan (Barbaria et al., 2025).

Teknologi *Blockchain* juga memungkinkan transparansi dan verifikasi yang lebih baik dalam proses audit. Auditor eksternal dapat memverifikasi integritas dari audit trail dan memastikan bahwa semua aktivitas telah dicatat dengan benar. Namun, implementasi *Blockchain* juga menghadapi tantangan termasuk skalabilitas, konsumsi energi, dan kompleksitas teknis. Organisasi harus mempertimbangkan dengan hati-hati apakah *Blockchain* cocok untuk kasus penggunaan mereka (Cadet et al., 2024).

8.4.4 Integrasi dengan Sistem Manajemen Risiko Perusahaan

Sistem audit dan kepatuhan perlindungan data harus terintegrasi dengan sistem manajemen risiko perusahaan yang lebih

luas. Ini memastikan bahwa risiko perlindungan data dipertimbangkan dalam konteks risiko perusahaan keseluruhan dan bahwa respons terhadap risiko selaras di seluruh organisasi. Integrasi dengan sistem GRC (*Governance, Risk, and Compliance*) memungkinkan organisasi untuk memiliki pandangan holistik tentang postur kepatuhan mereka (Oladosu et al., 2021).

Sistem terintegrasi juga memfasilitasi komunikasi yang lebih baik antara tim keamanan informasi, tim kepatuhan, dan manajemen puncak. Data dari sistem monitoring dan audit dapat disajikan dalam dasbor yang mudah dipahami yang menunjukkan status kepatuhan real-time. Ini membantu manajemen membuat keputusan berdasarkan informasi tentang investasi dalam keamanan data dan memastikan bahwa risiko ditangani dengan cepat (Goyal et al., 2025).

8.5 Respons Insiden dan Manajemen Pelanggaran Data

8.5.1 Perencanaan dan Respons Insiden Keamanan Data

Perencanaan respons insiden yang komprehensif adalah bagian penting dari program keamanan data. Rencana ini harus mendefinisikan langkah-langkah yang akan diambil ketika insiden keamanan terdeteksi, termasuk deteksi awal, investigasi, penghentian, pemulihan, dan pembelajaran pasca-insiden. Rencana harus jelas menetapkan peran dan tanggung jawab dari berbagai anggota tim, termasuk tim keamanan, manajemen, hukum, dan komunikasi (Bellala, 2025).

Respons insiden yang cepat dan efektif sangat penting untuk meminimalkan kerusakan dari pelanggaran data. Organisasi harus memiliki prosedur untuk segera mengisolasi sistem yang terkena dampak, melestarikan bukti untuk investigasi, dan mencegah penularan lebih lanjut. Tim respons insiden harus terdiri dari individu yang terlatih dan berpengalaman dalam menangani insiden keamanan data. Latihan simulasi insiden harus dilakukan secara berkala untuk memastikan kesiapan tim (Joodala, 2025).

8.5.2 Investigasi Pelanggaran Data dan Forensik Digital

Investigasi pelanggaran data melibatkan analisis menyeluruh tentang apa yang terjadi, bagaimana pelanggaran terjadi, siapa yang terlibat, dan data mana yang terkena dampak. Investigasi harus dilakukan dengan hati-hati untuk mempertahankan integritas bukti dan memastikan bahwa temuan dapat digunakan dalam tindakan hukum jika perlu. Forensik digital digunakan untuk menganalisis sistem yang terkompromi, mengidentifikasi titik masuk penyerang, dan melacak tindakan penyerang (Rachapalli, 2022).

Organisasi harus bekerja dengan spesialis forensik eksternal jika diperlukan dan melibatkan pihak hukum ketika ada kemungkinan pertanggungjawaban hukum. Dokumentasi yang teliti dari proses investigasi sangat penting untuk memastikan kredibilitas temuan dan untuk memenuhi persyaratan regulasi. Hasil investigasi harus digunakan untuk memperbaiki kontrol keamanan dan mencegah insiden serupa di masa depan (Barbaria et al., 2025).

8.5.3 Notifikasi Pelanggaran Data dan Kewajiban Regulasi

Regulasi seperti GDPR dan HIPAA mengharuskan organisasi untuk melaporkan pelanggaran data kepada otoritas pengawas dan individu yang terkena dampak dalam waktu yang ditentukan. GDPR memerlukan notifikasi kepada otoritas perlindungan data dalam 72 jam setelah pelanggaran ditemukan, dan pemberitahuan kepada individu harus dilakukan "tanpa penundaan yang tidak perlu" ketika ada risiko tinggi terhadap hak dan kebebasan mereka. Tidak mematuhi persyaratan notifikasi dapat mengakibatkan denda tambahan (Goyal et al., 2025).

Proses notifikasi harus dirancang dengan cermat untuk memberikan informasi yang akurat dan berguna kepada individu yang terkena dampak. Notifikasi harus mencakup penjelasan tentang apa yang terjadi, data mana yang terpengaruh, langkah-langkah yang sedang diambil untuk mengatasi pelanggaran, dan langkah-langkah yang dapat diambil oleh individu untuk melindungi diri mereka sendiri. Organisasi juga harus menyiapkan komunikasi untuk media dan pemangku kepentingan lain untuk mengelola reputasi mereka (Bakare et al., 2024).

8.5.4 Pembelajaran Pasca-Insiden dan Perbaikan Berkelanjutan

Setelah mengatasi insiden keamanan data, organisasi harus melakukan analisis menyeluruh untuk memahami penyebab akar dari pelanggaran dan mengidentifikasi pelajaran yang dapat diterapkan untuk mencegah insiden serupa di masa depan. Laporan pasca-insiden (*post-incident review*) harus didokumentasikan dan dibagikan dengan tim yang relevan. Temuan dari laporan ini harus

digunakan untuk memperbarui rencana respons insiden, memperbaiki kontrol keamanan, dan meningkatkan pelatihan karyawan (Garg, 2024).

Pembelajaran pasca-insiden juga harus melibatkan evaluasi tentang seberapa baik rencana respons insiden dijalankan dan area mana yang dapat ditingkatkan. Organisasi harus secara konsisten menggunakan pengalaman dari insiden untuk meningkatkan postur keamanan data mereka secara keseluruhan. Perbaikan yang diidentifikasi harus diimplementasikan dengan prioritas berdasarkan tingkat risiko, dan kemajuan dalam implementasi harus dilacak dan dilaporkan (Cadet et al., 2024).

Latihan Soal Essay

1. Jelaskan bagaimana Anda akan merancang program audit perlindungan data untuk organisasi kesehatan yang menangani data pasien sensitif. Program harus mencakup frekuensi audit, ruang lingkup, metodologi, dan bagaimana temuan audit akan ditindaklanjuti.
2. Diskusikan bagaimana teknologi dapat digunakan untuk mengimplementasikan sistem pengawasan berkelanjutan perlindungan data. Jelaskan komponen-komponen utama sistem ini, termasuk logging, deteksi anomali, dan pelaporan real-time, serta manfaat dan tantangan implementasinya.
3. Analisis tantangan yang dihadapi organisasi multinasional dalam mencapai kepatuhan terhadap regulasi perlindungan data yang berbeda (seperti GDPR, HIPAA, dan CCPA). Bagaimana strategi kepatuhan dapat diselaraskan untuk memenuhi persyaratan dari berbagai yurisdiksi?
4. Jelaskan langkah-langkah yang harus diambil organisasi ketika menemukan pelanggaran keamanan data, mulai dari deteksi awal hingga notifikasi kepada individu yang terkena dampak. Apa saja persyaratan regulasi yang harus dipenuhi dalam proses ini?
5. Diskusikan bagaimana organisasi dapat menggunakan hasil audit dan monitoring berkelanjutan untuk secara konsisten meningkatkan program kepatuhan perlindungan data mereka. Apa saja metrik kunci yang harus dilacak untuk mengukur efektivitas program kepatuhan?

DAFTAR PUSTAKA

Adepoju, D. A., & Adepoju, A. G. (2025). Establishing ethical frameworks for scalable data engineering and governance in AI-driven healthcare systems. *International Journal of Scientific & Engineering Research*, 6(4), 1547. **https://doi.org/10.55248/gengpi.6.0425.1547**

Ahmed, A., Shahzad, A., Naseem, A., Ali, S., & Ahmad, I. (2025). Evaluating the effectiveness of data governance frameworks in ensuring security and privacy of healthcare data: A quantitative analysis of ISO standards, GDPR, and HIPAA in *Blockchain* technology. *PLOS ONE*, 20(5), e0324285. **https://doi.org/10.1371/journal.pone.0324285**

Amadi, C. (2023). Ensuring HIPAA, CMS, and Joint Commission compliance by embedding governance structures, auditing mechanisms, and cross-disciplinary accountability systems. *International Journal of Scientific Research and Advanced Engineering*, 10(2), 952. **https://doi.org/10.30574/ijsra.2023.10.2.0952**

Barbaria, S., Jemai, A., Ceylan, H. I., Muntean, R., Dergaa, I., & Rahmouni, H. B. (2025). Advancing compliance with HIPAA and GDPR in healthcare: A *Blockchain*-based strategy for secure data exchange in clinical research involving private health information. *Healthcare*, 13(20), 2594. **https://doi.org/10.3390/healthcare13202594**

Bakare, S. S., Adeniyi, A. O., Akpuokwe, C. U., & Eneh, N. E. (2024). Data privacy laws and compliance: A comparative review of the EU GDPR and USA regulations. *CSI Transactions on ICT Research and Development*, 5(3), 859. **https://doi.org/10.51594/csitrj.v5i3.859**

Boadu, R. O., Adu, V. W., Okyere Boadu, K. A., Ibrahim, B., Akey, P., Mensah, A. A., ... & Mensah, N. K. (2025). Examine frameworks policies and strategies for effective information governance in healthcare organizations. *PLOS ONE*, 20(7), e0327496. **https://doi.org/10.1371/journal.pone.0327496**

Cadet, E., Babatunde, L. A., Ajayi, J. O., Erigh, E. D., Obuse, E., Essien, I. A. E., & Ayanbode, N. (2024). Developing scalable compliance architectures for cross-industry regulatory alignment. *International Journal of Scientific Research and Social Sciences*, 24(25), 56. **https://doi.org/10.32628/ijsrssh242556**

Conduah, A. K., Ofoe, S., & Siaw-Marfo, D. (2025). Data privacy in healthcare: Global challenges and solutions. *Sage Open Nursing*, 11(5), 1343959. **https://doi.org/10.1177/20552076251343959**

Edulakanti, N. (2025). Data governance frameworks for large-scale healthcare systems: A comparative study. *Journal of Information Systems, Engineering & Management*, 10(52), 10802. **https://doi.org/10.52783/jisem.v10i52s.10802**

Gadve, S., & Soni, G. (2025). Design and development of a privacy-preserving health record exchange framework using *Blockchain* for smart healthcare. In *2025 IEEE International Conference on Intelligent Communication and Computing Networks* (pp. 11232615). IEEE. **https://doi.org/10.1109/ICICNCT66124.2025.11232615**

Garg, V. (2024). Modern data governance technologies and their role in regulatory compliance: A study on GDPR and HIPAA. *International Scientific Journal of Engineering and Management*, 27(6), 0276. **https://doi.org/10.55041/isjem0276**

Goyal, A., Pendyala, J. P., & Bhat, R. (2025). Towards an AI framework for scalable compliance monitoring in regulated sectors. In *2025 IEEE International Conference on Computer Communications and Network Protocols* (pp. 11233371). IEEE. **https://doi.org/10.1109/ICCCNP63914.2025.11233371**

Idoko, B., Alakwe, J. A., Ugwu, O. J., Idoko, J. E., Idoko, F. O., Ayoola, V. B., ... & Adeyinka, T. (2024). Enhancing healthcare data privacy and security: A comparative study of regulations and best practices in the US and Nigeria. *Mathematical Statistical Research and Review*, 11(2), 110. **https://doi.org/10.30574/msarr.2024.11.2.0110**

Nangi, P. R., & Obannagari, C. K. R. N. (2025). AI-driven security automation for continuous compliance monitoring in regulated cloud environments. *International Journal of Electronics and Telecommunications and Computer Science and Information Technology*, 6(2), 112. **https://doi.org/10.63282/3050-9246.ijetcsit-v6i2p112**

Raveendran, N. (2025). Technical review: How HIPAA, GDPR, and DMA apply to information retrieval systems. *Global Journal of Engineering and Technology Analysis*, 24(1), 0212. **https://doi.org/10.30574/gjeta.2025.24.1.0212**

Samala, S. (2025). Automating ITSM compliance (GDPR/SOC 2/HIPAA) in Jira workflows: A framework for high-risk industries. *International Journal of Data Science and Machine Learning*, 5(1), 14. **https://doi.org/10.55640/ijdsml-05-01-14**

Tiwari, S. (2025). Security-first data engineering: Best practices for compliance in healthcare and financial data pipelines. *Journal of Information Systems, Engineering & Management*, 10(61), 13438. **https://doi.org/10.52783/jisem.v10i61s.13438**

Verma, S. (2025). Cybersecurity compliance in the age of remote work: Challenges and solutions. *World Journal of Advanced Engineering Technology and Sciences*, 15(1), 0286. **https://doi.org/10.30574/wjaets.2025.15.1.0286**

BAB 9
PENANGANAN INSIDEN KEBOCORAN DATA DAN MITIGASI RISIKO

Edi Sugiarto, SKM.,M.Kes

9.1 Fondasi Kebijakan Penanganan Insiden Kebocoran Data

9.1.1 Pemahaman tentang Insiden Kebocoran Data dalam Organisasi Kesehatan

Insiden kebocoran data (*data breach*) merupakan peristiwa di mana informasi kesehatan yang terlindungi (*Protected Health Information* atau PHI) diakses, diubah, atau didistribusikan tanpa otorisasi yang tepat (Balogun et al., 2025). Dalam konteks organisasi kesehatan, kebocoran data dapat mencakup akses tidak sah terhadap catatan medis elektronik, pencurian informasi pasien, atau pengungkapan informasi pribadi pasien kepada pihak ketiga tanpa izin. Organisasi kesehatan menghadapi risiko kebocoran data yang terus meningkat, dengan penelitian menunjukkan bahwa lebih dari 80% kebocoran dalam sektor kesehatan disebabkan oleh insiden hacking atau teknologi informasi (Balogun, 2025).

Dampak dari kebocoran data dalam organisasi kesehatan sangat serius dan multidimensional. Pertama, terdapat dampak finansial yang signifikan, dengan rata-rata biaya kebocoran data

dalam sektor kesehatan mencapai $9.77 hingga $10.93 juta per insiden (Vuppala et al., 2025). Kedua, kebocoran data dapat menyebabkan kerusakan reputasi organisasi kesehatan, menurunkan kepercayaan pasien, dan memengaruhi loyalitas pasien terhadap layanan kesehatan. Ketiga, kebocoran data dapat mengakibatkan konsekuensi regulasi yang serius, termasuk denda yang besar berdasarkan pelanggaran HIPAA, HITECH Act, dan regulasi perlindungan data lainnya (Otorkpa et al., 2024).

9.1.2 Jenis-Jenis Insiden Kebocoran Data Kesehatan

Insiden kebocoran data dalam organisasi kesehatan dapat dikategorikan ke dalam beberapa jenis berdasarkan mekanisme dan sumbernya. Jenis pertama adalah *hacking atau IT incidents*, yang merupakan penyebab terbesar kebocoran data dalam kesehatan. Jenis ini mencakup akses tidak sah ke sistem informasi, pemanfaatan kerentanan perangkat lunak, dan serangan cyberattack seperti ransomware dan phishing (Balogun et al., 2025). Ransomware telah mengalami peningkatan sebesar 123% dalam beberapa tahun terakhir dan merupakan ancaman serius bagi kontinuitas operasi kesehatan.

Jenis kedua adalah ancaman dari dalam (*insider threats*), yang melibatkan karyawan atau pihak internal yang secara sengaja atau tidak sengaja menyebabkan kebocoran data. Insider threats termasuk pencurian data yang disengaja, akses data yang tidak perlu karena inisiatif pribadi yang tidak tepat, atau kelalaian dalam menangani data sensitif (Erukayenure et al., 2025). Jenis ketiga

adalah kesalahan manusia dan kelalaian, seperti pengiriman data ke alamat email yang salah, kehilangan perangkat yang berisi data sensitif, atau konfigurasi sistem yang tidak aman (Adedoyin et al., 2025).

Jenis keempat adalah serangan spesifik seperti phishing, *Distributed Denial of Service* (DDoS), *Man-in-the-Middle* (MitM) attacks, malware, dan *SQL injection* yang memanfaatkan kerentanan teknis sistem (Otorkpa et al., 2024). Jenis kelima adalah kerentanan dalam infrastruktur cloud dan sistem yang terhubung dengan Internet of Medical Things (IoMT), yang memungkinkan akses tidak sah dari jarak jauh (Khatun et al., 2024).

9.1.3 Kerangka Regulasi dan Kepatuhan (Compliance Framework)

Organisasi kesehatan di berbagai negara harus mematuhi berbagai kerangka regulasi untuk melindungi data kesehatan pasien. Di Amerika Serikat, kerangka utama adalah HIPAA (*Health Insurance Portability and Accountability Act*), yang mengatur privasi, keamanan, dan notifikasi pelanggaran informasi kesehatan (Abbasi & Smith, 2024). HIPAA mewajibkan organisasi kesehatan untuk menerapkan safeguard administratif, fisik, dan teknis untuk melindungi PHI.

Di Eropa, GDPR (*General Data Protection Regulation*) yang berlaku sejak Mei 2018 mengatur perlindungan data pribadi termasuk data kesehatan dengan standar yang sangat ketat (Gilbert & Gilbert, 2025). GDPR memerlukan organisasi untuk melakukan

penilaian dampak privasi, memberi pemberitahuan kepada otoritas dalam waktu 72 jam setelah mendeteksi kebocoran data, dan memiliki Data Protection Officer (*DPO*) (Balogun, 2025).

Kerangka internasional lainnya yang relevan mencakup HITECH Act (yang meningkatkan penalti HIPAA), NIST Cybersecurity Framework, ISO/IEC 27001 (standar keamanan informasi), dan standar khusus industri seperti HITRUST yang menggabungkan berbagai kerangka regulasi (Hanumanthaiah, 2024). Kepatuhan terhadap berbagai kerangka regulasi ini memerlukan investasi sumber daya yang signifikan dan merupakan prioritas strategis bagi organisasi kesehatan.

9.1.4 Penilaian Risiko dan Vulnerabilitas Awal

Sebelum mengembangkan strategi penanganan insiden, organisasi kesehatan harus melakukan penilaian risiko yang menyeluruh untuk mengidentifikasi aset yang penting, ancaman yang mungkin, kerentanan sistem, dan probabilitas serta dampak potensial dari setiap risiko (Kolaventi et al., 2024). Penilaian risiko ini harus dilakukan secara berkala dan diperbaharui ketika ada perubahan signifikan dalam infrastruktur IT atau lanskap ancaman.

Penilaian dapat dilakukan menggunakan berbagai metodologi, seperti ISO/IEC 27001 *risk matrix*, NIST SP 800-30 untuk panduan penilaian risiko, atau metodologi proprietary yang dikembangkan oleh organisasi (Aldosari, 2025). Hasil penilaian risiko harus dikomunikasikan kepada stakeholder utama, termasuk manajemen senior, untuk mendapatkan dukungan dan alokasi

sumber daya yang diperlukan untuk mitigasi risiko (Komaragiri et al., 2025).

9.2 Deteksi dan Respons Awal Terhadap Insiden

9.2.1 Sistem Deteksi dan Monitoring Berkelanjutan

Deteksi dini terhadap insiden kebocoran data adalah kunci untuk meminimalkan dampak dan waktu *containment*. Organisasi kesehatan harus menerapkan sistem monitoring keamanan yang komprehensif untuk mendeteksi aktivitas yang mencurigakan secara real-time. Sistem ini mencakup *Security Information and Event Management* (SIEM), yang mengumpulkan dan menganalisis log keamanan dari berbagai sistem untuk mengidentifikasi pola serangan (Abdi et al., 2024).

Teknologi deteksi lanjutan seperti deteksi anomali berbasis *machine learning* dapat mengidentifikasi perilaku yang tidak biasa dalam aktivitas jaringan, akses data, atau penggunaan sistem (Adesokan-Imran et al., 2025). Model *machine learning* yang dilatih dengan baik dapat mencapai akurasi 92.7% dalam mengidentifikasi ancaman cybersecurity. Selain itu, organisasi kesehatan harus menerapkan monitoring untuk mengidentifikasi upaya *phishing*, malware, dan intrusi sistem (Nifakos et al., 2021).

Monitoring berkelanjutan juga harus mencakup pemeriksaan terhadap perangkat yang terhubung dengan jaringan kesehatan, termasuk *Internet of Medical Things* (IoMT) devices, untuk

memastikan bahwa tidak ada perangkat yang dikompromikan atau tidak sah terhubung dengan sistem (Kolo, 2025).

9.2.2 Protokol Identifikasi dan Eskalasi Insiden

Ketika aktivitas mencurigakan terdeteksi, organisasi kesehatan harus memiliki protokol yang jelas untuk mengidentifikasi apakah ini merupakan insiden keamanan yang sebenarnya atau hanya false positive (Balogun et al., 2025). Protokol ini harus mencakup investigasi awal untuk mengumpulkan informasi tentang sifat aktivitas, sistem yang terpengaruh, dan potensi dampak.

Jika aktivitas dikonfirmasi sebagai insiden keamanan, protokol eskalasi harus diaktifkan untuk menginformasikan stakeholder utama, termasuk *Chief Information Security Officer* (CISO), Chief Executive Officer (CEO), Chief Medical Officer (CMO), dan *Incident Response Team* (Burrell et al., 2026). Eskalasi ini harus mengikuti hirarki yang telah ditetapkan, dengan komunikasi yang jelas tentang tingkat keparahan insiden dan tindakan yang diperlukan.

9.2.3 Aktivasi Tim Respons Insiden

Tim respons insiden (*Incident Response Team*) harus diaktifkan segera setelah insiden diidentifikasi. Tim ini biasanya terdiri dari individu dari berbagai departemen, termasuk IT Security, Legal/Compliance, Medical Information, Administration, dan Communications (Shaik, 2025). Setiap anggota tim harus memiliki peran dan tanggung jawab yang jelas, dengan pemimpin tim yang ditunjuk untuk mengkoordinasikan respons.

Tim respons harus memiliki akses ke informasi yang diperlukan untuk melakukan investigasi, seperti log sistem, catatan akses, dan dokumentasi infrastruktur IT (Ekott et al., 2026). Tim juga harus memiliki wewenang untuk mengambil keputusan cepat, seperti mengisolasi sistem yang terpengaruh atau menutup akun yang mungkin dikompromikan, untuk menghentikan penyebaran insiden.

9.2.4 Komunikasi Darurat dan Notifikasi Internal

Komunikasi internal yang cepat dan akurat sangat penting dalam tahap awal respons insiden. Protokol komunikasi harus ditetapkan sebelumnya, termasuk siapa yang harus diberitahu, melalui saluran komunikasi apa, dan dalam format pesan apa (Ekott et al., 2026). Komunikasi harus mencakup informasi tentang sifat insiden, sistem yang terpengaruh, tindakan yang sedang diambil, dan instruksi untuk staf tentang cara merespons jika mereka menerima pertanyaan dari pasien atau media.

Organisasi kesehatan harus juga memastikan bahwa komunikasi internal tidak secara tidak sengaja mengungkapkan informasi sensitif tentang insiden kepada pihak luar, yang dapat memperburuk situasi. Oleh karena itu, komunikasi harus dibatasi hanya kepada individu yang perlu mengetahui dan menggunakan saluran komunikasi yang aman (Gumusel et al., 2024).

9.3 Investigasi Mendalam dan Analisis Forensik

9.3.1 Pengumpulan Bukti dan Preservasi Data

Investigasi forensik yang tepat memerlukan pengumpulan bukti yang cermat dan preservasi data untuk memastikan integritas bukti dan mendukung kemungkinan tindakan hukum atau peraturan di kemudian hari (Deshmukh & Shrivastav, 2024). Organisasi kesehatan harus memiliki protokol yang jelas untuk menangani dan mendokumentasikan semua bukti, termasuk log sistem, file, email, dan perangkat yang terpengaruh.

Bukti harus dikumpulkan dengan cara yang meminimalkan perubahan pada sistem dan menjaga *chain of custody* yang jelas. Tim respons harus mendokumentasikan siapa yang mengakses bukti, kapan, dan untuk tujuan apa. Bukti fisik, seperti hard drive atau perangkat jaringan, harus disimpan dengan aman dan dilindungi dari akses tidak sah (Idoko et al., 2024).

9.3.2 Analisis Akar Penyebab Insiden

Setelah bukti dikumpulkan, tim respons harus melakukan analisis akar penyebab (*root cause analysis*) untuk memahami bagaimana insiden terjadi, sistem mana yang dipengaruhi, dan data apa yang mungkin telah diakses atau dicuri. Analisis akar penyebab melibatkan pemeriksaan log sistem, dokumentasi keamanan, dan rekonstruksi kronologi peristiwa yang mengarah ke insiden (Balogun, 2025).

Hasil analisis akar penyebab harus dikomunikasikan kepada tim manajemen untuk membantu mereka memahami kerentanan yang memungkinkan insiden terjadi dan langkah-langkah apa yang harus diambil untuk mencegah insiden serupa di masa

depan (Adesokan-Imran et al., 2025). Analisis juga harus mengidentifikasi apakah insiden ini terisolasi atau bagian dari serangan yang lebih luas.

9.3.3 Penentuan Lingkup dan Dampak Insiden

Penentuan lingkup dan dampak insiden melibatkan identifikasi berapa banyak catatan pasien yang terpengaruh, informasi apa yang mungkin diakses atau dicuri, berapa banyak individu yang terpengaruh, dan sistem mana yang terkena dampak (Balogun et al., 2025). Organisasi kesehatan harus memiliki proses yang transparan dan metodis untuk menentukan lingkup, karena ini akan memengaruhi keputusan tentang notifikasi, komunikasi publik, dan investigasi regulasi.

Organisasi harus menggunakan berbagai sumber informasi untuk menentukan dampak, termasuk log akses, audit trail sistem, dan hasil analisis forensik (Adedoyin et al., 2025). Dalam beberapa kasus, mungkin sulit untuk menentukan dengan pasti apakah data tertentu diakses atau dicuri, dan organisasi mungkin perlu menggunakan penilaian profesional untuk membuat keputusan konservatif demi keamanan pasien.

9.3.4 Dokumentasi Temuan dan Laporan Investigasi

Semua temuan dari investigasi harus didokumentasikan secara menyeluruh dalam laporan investigasi yang komprehensif. Laporan ini harus mencakup timeline kejadian, analisis akar penyebab, penjelasan tentang lingkup dan dampak insiden, dan rekomendasi untuk tindakan pencegahan di masa depan (Gumusel et

al., 2024). Laporan harus disiapkan dengan hati-hati, karena mungkin diperlukan dalam prosiding hukum atau pemeriksaan regulasi.

Dokumentasi juga harus mencakup informasi tentang sistem atau proses yang gagal dan berkontribusi pada insiden, sehingga organisasi kesehatan dapat mempelajari pelajaran dan meningkatkan postur keamanan mereka (Abdukarimova, 2025). Laporan investigasi harus disimpan dengan aman dan hanya dapat diakses oleh individu yang berwenang.

9.4 Strategi Mitigasi dan Remediasi Risiko

9.4.1 Penghentian dan Pembatasan Insiden (Containment)

Tujuan utama dari *containment* adalah menghentikan penyebaran insiden dan mencegah akses lebih lanjut ke data yang terpengaruh. Strategi *containment* dapat mencakup isolasi sistem yang terpengaruh dari jaringan, menutup akun pengguna yang mungkin dikompromikan, atau mengubah kredensial akses (Balogun et al., 2025). Keputusan tentang strategi *containment* harus mempertimbangkan keseimbangan antara menghentikan insiden dan mempertahankan kontinuitas layanan kesehatan.

Organisasi kesehatan harus memiliki rencana *containment* yang telah disiapkan sebelumnya, yang mempertimbangkan berbagai skenario insiden dan dampaknya terhadap operasi layanan kesehatan (Burrell et al., 2026). Rencana

harus mencakup kriteria untuk mengambil keputusan *containment*, pihak yang berwenang untuk membuat keputusan, dan prosedur untuk mengimplementasikan tindakan *containment* dengan cepat.

9.4.2 Remediasi Sistem dan Restorasi Data

Setelah insiden terkontrol, organisasi kesehatan harus fokus pada remediasi sistem untuk menghapus malware, menutup kerentanan yang dieksploitasi, dan memulihkan sistem ke keadaan yang aman (Idoko et al., 2024). Proses remediasi dapat mencakup patching sistem, upgrade perangkat lunak, instalasi program antimalware, dan pengkonfigurasi ulang sistem keamanan.

Dalam beberapa kasus, organisasi kesehatan mungkin perlu memulihkan data dari backup untuk mengembalikan sistem ke keadaan sebelum insiden. Proses restorasi data harus dilakukan dengan hati-hati untuk memastikan bahwa data yang dipulihkan tidak mengandung malware atau modifikasi yang tidak sah (Thawbaan et al., 2025). Organisasi kesehatan harus juga menguji sistem yang dipulihkan secara menyeluruh sebelum mengembalikannya ke produksi untuk memastikan bahwa sistem berfungsi dengan benar dan tidak ada ancaman keamanan yang tersisa.

9.4.3 Implementasi Teknologi Mitigasi Lanjutan

Organisasi kesehatan harus menerapkan teknologi mitigasi lanjutan untuk memperkuat postur keamanan mereka dan mencegah insiden serupa di masa depan. Teknologi ini dapat mencakup *Zero*

Trust Architecture, yang menekankan verifikasi berkelanjutan dan akses dengan privilege minimum (Frimpong et al., 2025). Teknologi lainnya mencakup enkripsi data end-to-end, sistem autentikasi multi-faktor, dan sistem deteksi dan respons ancaman berbasis AI (V et al., 2025).

Organisasi kesehatan juga harus mempertimbangkan penggunaan *Blockchain* untuk menciptakan audit trail yang tidak dapat diubah dari semua akses dan modifikasi data kesehatan, serta untuk memfasilitasi konsultasi pasien yang aman dan terenkripsi (Barbaria et al., 2025). Teknologi mitigasi ini harus dipilih berdasarkan penilaian risiko spesifik organisasi dan harus terintegrasi dengan sistem yang ada dengan hati-hati.

9.4.4 Peningkatan Kontrol Keamanan dan Policy

Berdasarkan pembelajaran dari insiden, organisasi kesehatan harus memperbarui kebijakan keamanan, prosedur, dan kontrol untuk memperkuat pertahanan dan mencegah insiden serupa. Peningkatan dapat mencakup kebijakan akses yang lebih ketat, proses onboarding dan offboarding karyawan yang lebih baik, pelatihan keamanan yang lebih komprehensif, dan monitoring yang lebih ketat (Ogunyemi & Adetunji, 2025).

Organisasi kesehatan harus juga memastikan bahwa semua kontrol keamanan didokumentasikan dengan jelas, dikomunikasikan kepada semua staf yang relevan, dan secara teratur diaudit untuk kepatuhan (Zlatolas et al., 2024). Peningkatan kontrol keamanan

harus dilakukan dengan cara yang seimbang, mempertimbangkan dampak terhadap kegunaan sistem dan produktivitas staf.

9.5 Notifikasi, Komunikasi, dan Tanggung Jawab Hukum

9.5.1 Notifikasi Pasien dan Pihak Pihak Terkait

Organisasi kesehatan memiliki kewajiban hukum di bawah HIPAA, GDPR, dan regulasi lainnya untuk memberitahukan pasien dan pihak terkait lainnya dalam waktu yang ditentukan setelah mendeteksi kebocoran data yang melibatkan informasi pribadi (Abbasi & Smith, 2024). Notifikasi harus mencakup informasi tentang sifat kebocoran, jenis informasi yang terpengaruh, langkah-langkah yang diambil oleh organisasi kesehatan untuk mengatasi insiden, dan langkah-langkah yang dapat diambil pasien untuk melindungi diri mereka sendiri.

Notifikasi harus disampaikan dengan cara yang jelas, dapat dimengerti, dan dalam bahasa yang dapat diakses oleh pasien. Organisasi kesehatan juga harus menyediakan informasi tentang layanan monitoring kredit gratis atau layanan lain yang ditawarkan sebagai kompensasi untuk gangguan yang disebabkan oleh kebocoran (Gilbert & Gilbert, 2025). Waktu notifikasi sangat penting; GDPR memerlukan notifikasi kepada otoritas regulasi dalam waktu 72 jam, sementara beberapa negara memiliki persyaratan yang lebih ketat.

9.5.2 Komunikasi Publik dan Manajemen Reputasi

Selain notifikasi langsung kepada pasien, organisasi kesehatan mungkin perlu mengkomunikasikan insiden kepada publik dan media untuk mempertahankan kepercayaan dan transparansi (Ekott et al., 2026). Komunikasi publik harus disiapkan dengan hati-hati, menghindari overclaiming atau downplaying insiden, dan fokus pada langkah-langkah yang diambil untuk melindungi pasien dan mencegah insiden serupa di masa depan.

Organisasi kesehatan harus memiliki rencana komunikasi krisis yang telah disiapkan sebelumnya, yang mencakup siapa yang bertanggung jawab untuk komunikasi publik, pesan utama yang ingin disampaikan, dan saluran komunikasi yang akan digunakan (Abdukarimova, 2025). Komunikasi publik harus konsisten dengan notifikasi yang dikirimkan kepada pasien dan regulasi untuk menghindari kebingungan atau ketidakpercayaan.

9.5.3 Pelaporan Regulasi dan Kewajiban Compliance

Organisasi kesehatan harus melaporkan kebocoran data kepada otoritas regulasi yang relevan, seperti Office for Civil Rights (OCR) di bawah HIPAA, otoritas perlindungan data lokal di bawah GDPR, atau otoritas lain di negara tempat organisasi beroperasi (Ogunyemi & Adetunji, 2025). Laporan regulasi harus disertai dengan informasi terperinci tentang insiden, termasuk jenis data yang terkena, jumlah individu yang terpengaruh, dan langkah-langkah yang diambil untuk mencegah insiden serupa.

Organisasi kesehatan harus memastikan bahwa laporan regulasi dibuat dalam waktu yang ditentukan oleh hukum, karena keterlambatan dalam pelaporan dapat mengakibatkan denda tambahan atau tindakan enforcement oleh otoritas (Hanumanthaiah, 2024). Organisasi juga harus memastikan bahwa informasi yang dilaporkan akurat dan lengkap, karena informasi yang tidak akurat dapat mengakibatkan konsekuensi hukum tambahan.

9.5.4 Tanggung Jawab Hukum dan Pertimbangan Litigasi

Kebocoran data dapat mengakibatkan berbagai tanggung jawab hukum bagi organisasi kesehatan, termasuk denda regulasi di bawah HIPAA (hingga $1.5 juta per kategori pelanggaran per tahun), gugatan *class action* dari pasien yang dirugikan, dan tanggung jawab perdata (Balogun, 2025). Organisasi kesehatan harus bekerja dengan tim legal yang berpengalaman untuk mengembangkan strategi untuk meminimalkan tanggung jawab hukum dan menangani tuntutan yang mungkin timbul.

Dokumentasi yang cermat tentang investigasi insiden dan langkah-langkah yang diambil untuk mencegah insiden serupa sangat penting untuk membela organisasi kesehatan dalam litigasi (Gumusel et al., 2024). Organisasi harus juga mempertimbangkan untuk membeli asuransi *cyber liability* yang dapat membantu menutup biaya litigasi, denda, dan tanggung jawab lainnya yang mungkin timbul dari kebocoran data (Adedoyin et al., 2025).

9.6 Pembelajaran dan Perbaikan Berkelanjutan

9.6.1 Post-Incident Review dan Analisis Pembelajaran

Setelah insiden ditangani dan sistem dipulihkan, organisasi kesehatan harus melakukan review komprehensif tentang respons terhadap insiden untuk mengidentifikasi apa yang berjalan baik dan apa yang dapat ditingkatkan (Shaik, 2025). Review ini, sering disebut "post-incident review" atau "postmortem", harus melibatkan anggota dari tim respons insiden dan stakeholder utama lainnya.

Post-incident review harus menganalisis berbagai aspek respons insiden, termasuk kecepatan deteksi, efektivitas *containment*, kualitas komunikasi, dan keberhasilan remediasi (Burrell et al., 2026). Review juga harus mengidentifikasi area di mana kontrol keamanan gagal atau tidak efektif, dan merekomendasikan peningkatan untuk mencegah insiden serupa (Thawbaan et al., 2025). Pembelajaran dari insiden harus dibagikan secara luas dalam organisasi untuk meningkatkan kesadaran keamanan dan budaya keamanan.

9.6.2 Pembaruan Rencana Respons Insiden

Berdasarkan pembelajaran dari insiden, organisasi kesehatan harus memperbarui rencana respons insiden mereka untuk merefleksikan pengalaman dan perbaikan yang telah diidentifikasi (Deshmukh & Shrivastav, 2024). Rencana yang diperbarui harus mencakup prosedur yang lebih jelas, peran dan tanggung jawab yang lebih terdefinisi dengan baik, dan eskalasi yang lebih efektif.

Rencana respons insiden juga harus diperbarui secara berkala (setidaknya setiap tahun) untuk memastikan bahwa rencana tersebut tetap relevan dengan infrastruktur IT yang berubah, ancaman keamanan yang berkembang, dan perubahan regulasi (Suresh & Gummadi, 2025). Organisasi kesehatan harus melakukan latihan respons insiden secara berkala untuk memastikan bahwa tim respons siap untuk menangani insiden dengan efektif.

9.6.3 Pelatihan Keamanan dan Kesadaran Karyawan

Karena kesalahan manusia dan insider threats adalah penyebab utama kebocoran data dalam organisasi kesehatan, investasi dalam pelatihan keamanan dan kesadaran karyawan sangat penting (Erukayenure et al., 2025). Organisasi kesehatan harus memberikan pelatihan keamanan komprehensif kepada semua karyawan, dengan fokus khusus pada pengenalan phishing, manajemen password, dan handling data sensitif.

Pelatihan keamanan harus disesuaikan dengan peran spesifik karyawan, dengan pelatihan tambahan untuk staf IT dan keamanan (Nifakos et al., 2021). Organisasi kesehatan juga harus melakukan simulasi phishing secara berkala untuk menguji kesadaran karyawan dan mengidentifikasi karyawan yang memerlukan pelatihan tambahan (Arefin, 2024). Organisasi harus juga membangun budaya keamanan di mana karyawan merasa nyaman melaporkan aktivitas mencurigakan atau potensi kerentanan keamanan tanpa takut.

9.6.4 *Benchmarking* dan Penilaian Keamanan Berkelanjutan

Organisasi kesehatan harus secara berkala melakukan penilaian keamanan untuk mengukur efektivitas program keamanan mereka dan mengidentifikasi area untuk perbaikan (Aldosari, 2025). Penilaian dapat mencakup *vulnerability assessments*, *penetration testing*, *security audits*, dan penilaian kepatuhan regulasi (R et al., 2024). Hasil penilaian harus dibandingkan dengan benchmark industri untuk mengidentifikasi area di mana organisasi kesehatan tertinggal atau unggul dibandingkan dengan organisasi lain.

Organisasi kesehatan juga harus mengikuti perkembangan terbaru dalam ancaman keamanan, teknologi, dan best practices, dan memastikan bahwa program keamanan mereka tetap relevan dan efektif (Omotade et al., 2025). Investasi berkelanjutan dalam keamanan informasi adalah penting untuk mempertahankan postur keamanan yang kuat dan melindungi data pasien dari ancaman yang terus berkembang.

Latihan Soal

1. Anda adalah *Chief Information Security Officer* (CISO) di sebuah rumah sakit besar yang baru-baru ini mengalami kebocoran data yang melibatkan catatan medis elektronik 50,000 pasien. Jelaskan strategi mitigasi risiko komprehensif yang akan Anda implementasikan untuk mencegah insiden serupa di masa depan. Strategi harus mencakup teknologi, proses organisasi, dan elemen manusia. Berikan contoh spesifik tentang bagaimana setiap elemen strategi akan mengatasi kerentanan yang memungkinkan kebocoran terjadi.
2. Desain protokol deteksi dan respons insiden untuk organisasi kesehatan yang mencakup identifikasi awal, eskalasi, investigasi forensik, *containment*, dan remediasi. Jelaskan peran berbagai tim (IT Security, Legal, Medical Records, Administration, Communications) dalam setiap tahap respons. Bagaimana Anda akan memastikan bahwa protokol ini dapat diimplementasikan dengan cepat tanpa mengganggu layanan kesehatan yang kritis?
3. Jelaskan bagaimana organisasi kesehatan harus mengkomunikasikan kebocoran data kepada berbagai stakeholder, termasuk pasien, media, otoritas regulasi, dan karyawan. Apa yang harus dipertimbangkan dalam mengembangkan pesan komunikasi yang efektif? Bagaimana organisasi dapat mempertahankan kepercayaan dan transparansi sambil meminimalkan kerusakan reputasi?

4. Analisis kewajiban kepatuhan organisasi kesehatan di bawah HIPAA, GDPR, dan regulasi lokal lainnya dalam merespons kebocoran data. Jelaskan apa yang dimaksud dengan "notifikasi dalam waktu 72 jam", persyaratan investigasi, dan mekanisme pelaporan. Apa konsekuensi dari ketidaksesuaian dan bagaimana organisasi kesehatan dapat meminimalkan risiko hukum?
5. Jelaskan bagaimana organisasi kesehatan dapat membangun program keamanan informasi yang berkelanjutan, termasuk pelatihan karyawan, penilaian keamanan berkala, manajemen vendor, dan budaya keamanan. Bagaimana organisasi dapat menyeimbangkan kebutuhan keamanan dengan kebutuhan operasional dan inovasi dalam layanan kesehatan? Berikan contoh metrik atau KPI untuk mengukur efektivitas program keamanan.

DAFTAR PUSTAKA

Abbasi, N., & Smith, D. A. (2024). Cybersecurity in healthcare: Securing patient health information (PHI), HIPPA compliance framework and the responsibilities of healthcare providers. *Journal of King Saud University – Science and Technology*, 3(3), 278-287. **https://doi.org/10.60087/jklst.vol3.n3.p.278-287**

Abunadi, I., & Kumar, R. (2021). BSF-EHR: *Blockchain* security framework for electronic health records of patients. *Sensors*, 21(8), 2865. **https://doi.org/10.3390/s21082865**

Adesokan-Imran, T. O. (2025). The impact of cybersecurity governance on national security by strengthening critical infrastructure through IT auditing and risk management. *Asian Journal of Research in Computer Science*, 18(4), 4621. **https://doi.org/10.9734/ajrcos/2025/v18i4621**

Adesokan-Imran, T. O., Popoola, A. D., Ejiofor, V. O., Salako, A., & Onyenaucheya, O. (2025). Predictive cybersecurity risk modeling in healthcare by leveraging AI and machine learning for proactive threat detection. *Journal of Engineering Research and Reports*, 27(4), 1463. **https://doi.org/10.9734/jerr/2025/v27i41463**

Adesokan-Imran, T. O., Farinde, O., Ogunsola, O., Chiobi, N. F., & Akinola, O. (2025). Breach prevention strategies for cybersecurity in US SMEs and healthcare

organizations. *World Journal of Advanced Research and Reviews*, 26(2), 49. **https://doi.org/10.30574/wjarr.2025.26.2.0049**

Ahmed, W., Chowdhury, A., Fathima Shah, W., & Ali, M. (2025). AI and *Blockchain* for securing healthcare data: A framework for national health information systems. *International Journal of Data Science and Machine Learning*, 5(2), 11. **https://doi.org/10.55640/ijdsml-05-02-11**

Al Amin, M., Shah, R., Tummala, H., & Ray, I. (2025). Did you break the glass properly? A policy compliance framework for protected health information (PHI) emergency access. *Proceedings of the International Conference on Enterprise Information Systems*, 2013(2), 3979. **https://doi.org/10.5220/0013527000003979**

Al Amin, M., Tummala, H., Shah, R., & Ray, I. (2024). Balancing patient privacy and health data security: The role of compliance in protected health information (PHI) sharing. *Proceedings of the International Conference on Enterprise Information Systems*, 2012(1), 3767. **https://doi.org/10.5220/0012767400003767**

Aldosari, B. (2025). Cybersecurity in healthcare: New threat to patient safety. *Cureus*, 17(5), 83614. **https://doi.org/10.7759/cureus.83614**

Ali, M. (2025). Artificial intelligence in healthcare: Safeguarding data and enhancing information access through cybersecurity. *Georgian International Institute of Artificial Intelligence and Computer Science*, 1(2), 57-80. **https://doi.org/10.70445/giaic.1.2.2025.57-80**

Alugo, N. R. (2024). Data protection in the cloud: Ensuring security and compliance for organizational data. *International Journal for Research in Applied Science and Engineering Technology*, 12(12), 66087. **https://doi.org/10.22214/ijraset.2024.66087**

Arefin, S. (2024). Strengthening healthcare data security with AI-powered threat detection. *International Journal of Scientific Research and Management*, 12(10), EC02. **https://doi.org/10.18535/ijsrm/v12i10.ec02**

Avireneni, R. T. (2025). API-driven security and compliance in digital health infrastructure: Leveraging middleware for comprehensive protection of patient data. *International Journal of Computer Science and Information Technology*, 13(3), 4959. **https://doi.org/10.37745/ejcsit.2013/vol13n344959**

Balogun, A. Y. (2025). Enhancing incident response strategies in U.S. healthcare cybersecurity. *Journal of Engineering Research and Reports*, 27(2), 1399. **https://doi.org/10.9734/jerr/2025/v27i21399**

Balogun, A. Y. (2025). Strengthening compliance with data privacy regulations in U.S. healthcare cybersecurity. *Asian Journal of Research in Computer Science*, 18(1), 1555. **https://doi.org/10.9734/ajrcos/2025/v18i1555**

Barbaria, S., Jemai, A., Ceylan, H. I., Muntean, R., Dergaa, I., & Rahmouni, H. B. (2025). Advancing compliance with HIPAA and GDPR in healthcare: A *Blockchain*-based strategy for secure data exchange in clinical research involving private health information. *Healthcare*, 13(20), 2594. **https://doi.org/10.3390/healthcare13202594**

Benacerraf-Bezalel, M., Abdi, A., Bennouri, H., & Keane, A. (2024). Emerging cyber risks & threats in healthcare systems: A case study in resilient cybersecurity solutions. *2024 IEEE 6th International Conference on Electrical Engineering and Control Applications (MECO)*, 10577790. **https://doi.org/10.1109/meco62516.2024.10577790**

Burrell, D., Burton, S., Jones, L. A., Nobles, C., & Dawson, M. E. (2026). Healthcare administration in the age of complex dynamics in hospital and health system cybersecurity risk mitigation. *British Journal of Business and Venture*, 8(1), 015. **https://doi.org/10.34140/bjbv8n1-015**

Chevuri, N. K. (2025). Data protection in social services: A comprehensive guide to HIPAA and GDPR implementation. *Computer Science and Engineering*

Information Technology, 25(1), 2369. **https://doi.org/10.32628/cseit25112369**

Di Palma, G., Scendoni, R., Ferorelli, D., De Benedictis, A., Tambone, V., & De Micco, F. (2025). AI-induced cybersecurity risks in healthcare: A narrative review of *Blockchain*-based solutions within a clinical risk management framework. *

BAB 10
IMPLEMENTASI KEAMANAN DATA DI BERBAGAI LAYANAN KESEHATAN

Muhammad Rifqi Aufa Daffa, A.Md.Kes

10.1 Dasar-Dasar Keamanan Data Kesehatan

10.1.1 Pengertian dan Pentingnya Keamanan Data Kesehatan

Keamanan data kesehatan merupakan fondasi penting dalam sistem layanan kesehatan modern yang terintegrasi dengan teknologi digital. Dalam era transformasi digital, data kesehatan pasien mencakup informasi sensitif seperti riwayat medis, hasil laboratorium, resep obat, dan identitas personal yang harus dilindungi dengan standar keamanan tertinggi (Ikawati & Haris, 2024). Pentingnya keamanan data kesehatan tidak hanya terletak pada perlindungan privasi pasien, tetapi juga pada menjaga integritas informasi medis yang akan digunakan untuk pengambilan keputusan klinis. Ketika data kesehatan dikompromikan, dampaknya dapat mencakup risiko diagnosis yang salah, pengobatan yang tidak tepat, dan bahkan mengancam keselamatan pasien secara langsung.

Keamanan data dalam konteks layanan kesehatan melibatkan pelindungan data yang komprehensif di berbagai titik, mulai dari

pengumpulan data hingga penyimpanan dan akses. Implementasi keamanan data yang efektif memerlukan pemahaman mendalam tentang arsitektur sistem informasi kesehatan, ancaman keamanan siber yang spesifik terhadap sektor kesehatan, dan mekanisme perlindungan yang dapat diterapkan secara praktis. Setiap layanan kesehatan, baik itu rumah sakit, klinik, pusat kesehatan, maupun fasilitas telemedicine, memiliki karakteristik unik yang memengaruhi strategi implementasi keamanan data mereka (Makinde, 2025).

10.1.2 Komponen Utama Keamanan Data Kesehatan

Keamanan data kesehatan terdiri dari tiga pilar utama yang dikenal sebagai *confidentiality*, *integrity*, dan *availability* atau sering disebut sebagai prinsip CIA. *Confidentiality* atau kerahasiaan memastikan bahwa data hanya dapat diakses oleh pihak yang berwenang dan tidak disertakan kepada pihak yang tidak memiliki otorisasi. Hal ini dicapai melalui enkripsi data dan mekanisme kontrol akses yang ketat. *Integrity* atau integritas data berarti data harus tetap akurat, lengkap, dan tidak mengalami perubahan yang tidak sah selama penyimpanan, transmisi, atau pemrosesan. Sementara *availability* atau ketersediaan data mengacu pada kemampuan sistem untuk menyediakan akses data kepada pengguna yang berwenang kapan saja diperlukan (Shojaei et al., 2024).

Selain tiga pilar utama tersebut, terdapat komponen tambahan yang sama pentingnya dalam implementasi keamanan data kesehatan. *Authentication* atau autentikasi memastikan bahwa

pengguna yang mengakses sistem adalah benar-benar siapa mereka klaim. Mekanisme ini dapat diimplementasikan melalui kombinasi nama pengguna dan kata sandi, sertifikat digital, atau bahkan biometrik. *Non-repudiation* atau ketidakingkaran memastikan bahwa pengguna tidak dapat menyangkal telah melakukan suatu tindakan terhadap data. Komponen terakhir adalah *audit trail*, yang merupakan catatan lengkap tentang setiap aktivitas yang dilakukan terhadap data kesehatan, memungkinkan pelacakan dan penyelidikan jika terjadi insiden keamanan.

10.1.3 Jenis-Jenis Data Kesehatan yang Perlu Dilindungi

Data kesehatan yang memerlukan perlindungan keamanan dapat dibagi menjadi beberapa kategori berdasarkan sifat dan sensitifitasnya. *Electronic Health Records* atau catatan kesehatan elektronik merupakan representasi digital dari riwayat medis pasien yang mencakup diagnosis, pengobatan, hasil laboratorium, dan catatan klinis. Data ini dianggap sangat sensitif karena mengandung informasi medis lengkap tentang kondisi kesehatan pasien. *Protected Health Information* atau informasi kesehatan yang terlindungi mencakup data demografis pasien seperti nama, tanggal lahir, alamat, nomor identitas, dan informasi asuransi kesehatan yang ketika dikombinasikan dengan data medis dapat mengidentifikasi individu (Abbasi & Smith, 2024).

Selain data pasien, terdapat jenis data kesehatan lainnya yang memerlukan perlindungan seperti data administratif rumah sakit, informasi farmasi, data laboratorium, hasil *imaging* medis, dan data

keuangan kesehatan. Setiap jenis data memiliki tingkat sensitivitas dan persyaratan keamanan yang berbeda. Misalnya, hasil tes genetik memiliki implikasi privasi yang lebih luas dibandingkan catatan janji temu biasa, karena dapat mengungkap informasi tentang keluarga pasien. Data imaging medis seperti sinar-X dan MRI memerlukan penyimpanan dengan kapasitas besar dan mekanisme akses yang terkontrol dengan baik untuk memastikan hanya tenaga medis yang berwenang yang dapat mengaksesnya.

Fasilitas pelayanan kesehatan dalam hal ini rumah sakit memiliki kewajiban melindungi data dan informasi pasien maupun rumah sakit. Seperti yang dijelaskan dalam Instrumen Survei Akreditasi Rumah Sakit Nomor HK.02.02/D/47104/2024 dalam Standar MRMIK 2.2 dijelaskan bahwa Rumah Sakit menjaga kerahasiaan, keamanan, privasi, integritas data dan informasi melalui proses yang melindungi data dan informasi dari kehilangan, pencurian, kerusakan, dan penghancuran.

10.1.4 Ancaman Keamanan dalam Layanan Kesehatan

Layanan kesehatan menghadapi berbagai jenis ancaman keamanan yang terus berkembang seiring dengan kemajuan teknologi. *Cyberattack* atau serangan siber termasuk upaya dari pihak luar untuk mendapatkan akses tidak sah ke sistem kesehatan dengan tujuan mencuri data, merusak sistem, atau mengganggu layanan. *Ransomware* merupakan jenis malware yang mengenkripsi data pasien dan mengancam menghapusnya jika tidak ada pembayaran uang tebusan dilakukan. Ancaman ini telah terbukti

sangat merugikan bagi institusi kesehatan, menyebabkan gangguan layanan medis dan kerugian finansial yang signifikan.

Ancaman lainnya mencakup *insider threats* atau ancaman dari dalam, yang berasal dari karyawan atau staf kesehatan yang menyalahgunakan akses mereka untuk mengakses data pasien secara ilegal. *Phishing* dan *social engineering* merupakan teknik manipulasi yang memanfaatkan kelemahan manusia untuk mendapatkan akses atau informasi sensitif. Selain itu, terdapat ancaman teknis seperti kerentanan dalam aplikasi, sistem operasi yang belum diperbarui, dan infrastruktur jaringan yang lemah. Pemahaman komprehensif tentang berbagai jenis ancaman ini adalah langkah pertama dalam merancang strategi keamanan data yang efektif untuk layanan kesehatan (Makinde, 2025).

10.2 Implementasi Teknologi dalam Keamanan Data Kesehatan

10.2.1 Enkripsi dan Mekanisme Perlindungan Data

Enkripsi merupakan teknologi fundamental dalam melindungi data kesehatan dari akses tidak sah. Enkripsi berfungsi dengan mengubah data asli menjadi bentuk terenkripsi yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai. Dalam layanan kesehatan, enkripsi diimplementasikan pada dua tingkat utama: enkripsi data saat transit (*data in transit*) dan enkripsi data saat penyimpanan (*data at rest*). Enkripsi data saat transit melindungi informasi kesehatan ketika ditransmisikan melalui jaringan, baik itu jaringan internal rumah sakit maupun internet. Enkripsi data saat

penyimpanan memastikan bahwa bahkan jika penyimpanan fisik dikompromikan, data tetap terlindungi (Gowthamani et al., 2025).

Terdapat berbagai algoritma enkripsi yang digunakan dalam sistem kesehatan, mulai dari *Advanced Encryption Standard* (AES) yang merupakan standar industri, hingga *Elliptic Curve Cryptography* (ECC) yang menawarkan keamanan dengan ukuran kunci yang lebih kecil. Pemilihan algoritma enkripsi harus mempertimbangkan keseimbangan antara tingkat keamanan yang diperlukan, kemampuan komputasi sistem, dan performa yang dapat diterima. Selain enkripsi simetris dan asimetris, terdapat juga mekanisme seperti *homomorphic encryption* yang memungkinkan komputasi dilakukan pada data terenkripsi tanpa perlu mendekripsi terlebih dahulu, memberikan lapisan keamanan tambahan untuk aplikasi analisis data kesehatan yang sensitive (D, 2024).

10.2.2 Sistem Manajemen Akses dan Autentikasi

Manajemen akses yang tepat merupakan komponen kritis dalam keamanan data kesehatan. *Role-Based Access Control* (RBAC) merupakan model kontrol akses yang umum diimplementasikan dalam sistem kesehatan, di mana setiap pengguna diberi peran spesifik (misalnya dokter, perawat, apoteker) dan setiap peran memiliki hak akses terhadap data tertentu. Model RBAC memastikan bahwa setiap staf kesehatan hanya dapat mengakses data yang relevan dengan fungsi pekerjaan mereka, meminimalkan risiko akses data yang tidak sesuai (A & Prasanna, 2024).

Sistem autentikasi multi-faktor (*multi-factor authentication* atau MFA) telah menjadi standar dalam implementasi keamanan modern. MFA menggabungkan minimal dua metode verifikasi identitas, seperti kata sandi (sesuatu yang diketahui), kartu akses (sesuatu yang dimiliki), dan biometrik (sesuatu yang dimiliki secara unik). Implementasi MFA secara signifikan meningkatkan keamanan sistem kesehatan dengan mengurangi risiko akses yang tidak sah bahkan jika kredensial pengguna dikompromikan. Selain itu, sistem pemantauan aktivitas pengguna dan *audit logging* membantu dalam mendeteksi dan menyelidiki penggunaan akses yang mencurigakan atau tidak sesuai (Riswaya & Wahyudi, 2025).

10.2.3 Teknologi *Blockchain* untuk Keamanan Data Kesehatan

Blockchain telah menjadi teknologi yang semakin populer dalam implementasi keamanan data kesehatan karena karakteristik inheren yang mendukung keamanan. *Blockchain* adalah buku besar terdesentralisasi yang mencatat transaksi dalam blok yang terhubung secara kriptografis, membuat data sangat sulit untuk diubah atau dimanipulasi. Dalam konteks kesehatan, *Blockchain* dapat digunakan untuk menciptakan catatan medis yang immutable dan transparan, memastikan integritas data dan memudahkan audit trail (D, 2024).

Implementasi *Blockchain* dalam sistem kesehatan dapat menggunakan dua pendekatan utama: *Blockchain* publik dan *Blockchain permissioned* atau *private*. *Blockchain* publik seperti

Ethereum memungkinkan siapa saja untuk berpartisipasi dalam jaringan, sementara *Blockchain permissioned* seperti Hyperledger Fabric membatasi partisipasi hanya untuk organisasi yang diizinkan. Untuk aplikasi kesehatan yang memerlukan privasi data pasien yang ketat, *Blockchain permissioned* lebih sesuai. Teknologi *smart contract* dalam *Blockchain* memungkinkan otomasi proses verifikasi dan otorisasi akses data, menambah lapisan keamanan dan efisiensi dalam manajemen data kesehatan (D, 2024).

10.2.4 Infrastruktur Cloud dan Keamanan Berbasis Cloud

Banyak layanan kesehatan modern mengadopsi infrastruktur cloud computing untuk penyimpanan dan pemrosesan data kesehatan. Platform cloud seperti *Google Cloud Platform* (GCP), *Amazon Web Services* (AWS), dan *Microsoft Azure* menyediakan berbagai fitur keamanan yang canggih, seperti enkripsi data, isolasi tenants, dan pemantauan keamanan real-time. Keuntungan menggunakan infrastruktur cloud termasuk skalabilitas, aksesibilitas dari berbagai lokasi, dan pembaruan keamanan yang dilakukan oleh penyedia cloud secara otomatis (A & Prasanna, 2024).

Selain itu, teknologi cloud memungkinkan integrasi data kesehatan antar fasilitas pelayanan kesehatan sehingga mendukung interoperabilitas sistem informasi kesehatan. Melalui pendekatan ini, rumah sakit, laboratorium, dan fasilitas kesehatan lainnya dapat berbagi data pasien secara lebih cepat dan efisien dengan tetap memperhatikan aspek kerahasiaan dan integritas data. Infrastruktur

cloud juga mendukung penerapan *big data analytics*, kecerdasan buatan (*artificial intelligence*), dan *machine learning* dalam analisis data kesehatan untuk meningkatkan kualitas pelayanan medis dan pengambilan keputusan klinis (Kumar & Singh, 2023).

Namun, penggunaan cloud juga memperkenalkan tanggung jawab keamanan bersama (*shared responsibility model*) antara penyedia cloud dan organisasi kesehatan. Organisasi kesehatan tetap bertanggung jawab untuk mengimplementasikan kontrol keamanan pada tingkat aplikasi dan data, serta memastikan kepatuhan terhadap regulasi privasi data. Implementasi solusi cloud hybrid, yang menggabungkan infrastruktur on-premise dan cloud, sering digunakan oleh organisasi kesehatan untuk menyeimbangkan keamanan, fleksibilitas, dan biaya. Selain itu, *edge computing* yang memproses data lebih dekat ke sumbernya juga diimplementasikan dalam beberapa sistem kesehatan untuk mengurangi latensi dan meningkatkan keamanan dengan meminimalkan transmisi data sensitif melalui jaringan publik.

Selain itu menurut Fauziah (2014) dalam Tinjauan Keamanan Sistem Pada Teknologi Cloud Computing, penggunaan cloud computing mempunyai banyak tantangan apabila organisasi berpindah ke layanan komputasi awan publik tentunya infrastruktur sistem komputasi dikendalikan oleh pihak ketiga yaitu Cloud Service Provider (CSP). Tantangan ini harus ditangani melalui inisiatif manajemen yang diperlukan gambaran jelas peran

kepemilikan dan tanggung jawab dari CSP dan organisasi berperan sebagai pelanggan.

Pencurian data dalam teknologi Cloud Computing merupakan salah satu isu keamanan yang cukup besar. Hal ini karena setiap hacker dapat menggunakan berbagai cara untuk mendapatkan informasi yang dibutuhkan dari suatu perusahaan tertentu. Ada beberapa cara untuk dapat mencegah hal ini dapat terjadi. Menurut Setiawan (2010), beberapa cara pencurian data dapat dilakukan dengan cara yaitu *Denial of Service, QoS Violation, IP Spoofing, Port Scanning, dan ARP Cache Attack* (Fauziah, 2014).

10.3 Standar dan Regulasi Keamanan Data Kesehatan

10.3.1 Peraturan HIPAA dan Kepatuhannya

Health Insurance Portability and Accountability Act (HIPAA) merupakan undang-undang federal Amerika Serikat yang menetapkan standar nasional untuk perlindungan privasi dan keamanan data kesehatan. HIPAA berlaku untuk organisasi kesehatan yang menyimpan, memproses, atau mentransmisikan informasi kesehatan yang terlindungi. Standar keamanan HIPAA mencakup tiga aspek utama: standar administratif, standar fisik, dan standar teknis. Standar administratif mencakup kebijakan dan prosedur organisasi, manajemen risiko, dan pelatihan staf. Standar fisik mengacu pada perlindungan fasilitas dan perangkat. Standar teknis mencakup kontrol akses, enkripsi, dan audit logging (Abbasi & Smith, 2024).

Kepatuhan terhadap HIPAA bukan hanya persyaratan hukum tetapi juga praktek terbaik dalam menjaga keamanan data kesehatan. Organisasi kesehatan yang tidak mematuhi HIPAA dapat dikenai denda yang sangat besar, mulai dari ribuan hingga jutaan dolar per pelanggaran. Lebih penting lagi, pelanggaran HIPAA dapat merusak reputasi organisasi dan mengurangi kepercayaan pasien. Implementasi kepatuhan HIPAA memerlukan program keamanan informasi yang komprehensif, termasuk penilaian risiko berkelanjutan, pelatihan karyawan yang teratur, dan rencana respons insiden yang solid (Abbasi & Smith, 2024).

10.3.2 Regulasi GDPR dan Standar Internasional Lainnya

General Data Protection Regulation (GDPR) merupakan regulasi Uni Eropa yang sangat ketat mengenai perlindungan data pribadi. GDPR berlaku tidak hanya untuk organisasi di Eropa tetapi juga untuk organisasi di luar Eropa yang memproses data warga Eropa. Dalam konteks layanan kesehatan, GDPR memberikan perlindungan yang sangat kuat terhadap data kesehatan pribadi, yang dianggap sebagai kategori data sensitif khusus. GDPR menetapkan prinsip-prinsip seperti transparansi, akuntabilitas, dan *privacy by design* yang harus diimplementasikan dalam sistem kesehatan.

Selain HIPAA dan GDPR, terdapat berbagai standar keamanan data kesehatan lainnya yang diakui secara internasional. *ISO/IEC 27001* merupakan standar internasional untuk manajemen keamanan informasi yang dapat diterapkan pada organisasi kesehatan. *ISO 13485* berfokus pada keamanan perangkat

medis, sementara *HL7 FHIR* (*Fast Healthcare Interoperability Resources*) adalah standar untuk pertukaran data kesehatan yang interoperabel dengan keamanan bawaan. Organisasi kesehatan global sering mengimplementasikan kombinasi standar ini untuk memastikan kepatuhan terhadap berbagai regulasi regional dan best practices industri (Shojaei et al., 2024).

10.3.3 Standar Nasional dan Regulasi Lokal

Berbagai negara telah mengembangkan standar dan regulasi nasional untuk keamanan data kesehatan yang sesuai dengan konteks hukum dan budaya lokal mereka. Indonesia, misalnya, memiliki berbagai peraturan terkait keamanan data kesehatan, termasuk Undang-Undang Perlindungan Data Pribadi, Peraturan Menteri Kesehatan mengenai catatan medis elektronik, dan standar keamanan informasi dari Badan Siber dan Sandi Negara. Implementasi regulasi lokal memerlukan pemahaman mendalam tentang persyaratan spesifik yang berlaku dalam yurisdiksi masing-masing (Ikawati & Haris, 2024).

Standar lokal sering kali lebih sesuai dengan infrastruktur dan kemampuan organisasi kesehatan di wilayah tersebut. Sebagai contoh, standar keamanan untuk rumah sakit di negara berkembang mungkin mempertimbangkan keterbatasan infrastruktur internet dan keterbatasan anggaran. Meskipun demikian, standar lokal tetap harus memastikan tingkat keamanan data yang memadai untuk melindungi pasien. Organisasi kesehatan yang beroperasi di berbagai yurisdiksi harus mengimplementasikan keamanan data

yang memenuhi standar tertinggi yang berlaku di mana saja mereka beroperasi untuk menghindari risiko kepatuhan (Ikawati & Haris, 2024).

10.3.4 Sertifikasi dan Audit Keamanan

Sertifikasi keamanan informasi menjadi bukti bahwa organisasi kesehatan telah mengimplementasikan standar keamanan yang diakui. Sertifikasi ISO/IEC 27001, SOC 2 (*Service Organization Control*), dan sertifikasi khusus kesehatan lainnya menunjukkan komitmen organisasi terhadap keamanan data. Sertifikasi ini diperoleh melalui audit independen yang menyeluruh dan memerlukan pemeliharaan berkelanjutan untuk memastikan kepatuhan yang berkelanjutan.

Audit keamanan, baik internal maupun eksternal, merupakan mekanisme penting untuk memvalidasi keefektifan kontrol keamanan yang telah diimplementasikan. Audit internal dilakukan oleh tim internal organisasi untuk mengevaluasi kepatuhan terhadap kebijakan keamanan, sementara audit eksternal dilakukan oleh pihak ketiga independen untuk memberikan penilaian yang objektif. *Penetration testing* atau uji penetrasi adalah praktik keamanan yang melibatkan simulasi serangan untuk mengidentifikasi kerentanan dalam sistem sebelum penyerang nyata dapat memanfaatkannya. Melalui kombinasi audit, sertifikasi, dan pengujian keamanan, organisasi kesehatan dapat terus meningkatkan postur keamanan mereka dan memastikan perlindungan data pasien yang optimal (Mathur et al., 2025).

10.4 Tantangan dan Strategi Implementasi Keamanan Data

10.4.1 Tantangan Teknis dalam Implementasi Keamanan

Implementasi keamanan data dalam layanan kesehatan menghadapi berbagai tantangan teknis yang kompleks. Salah satu tantangan utama adalah *interoperability* atau interoperabilitas antara sistem kesehatan yang berbeda. Banyak organisasi kesehatan menggunakan sistem informasi yang berbeda untuk berbagai fungsi (misalnya manajemen pasien, laboratorium, farmasi), dan sistem-sistem ini sering kali tidak dirancang untuk berkomunikasi secara aman. Mengintegrasikan sistem-sistem ini sambil mempertahankan keamanan data memerlukan middleware keamanan yang kompleks dan protokol enkripsi yang robust (Ikawati & Haris, 2024).

Tantangan teknis lainnya mencakup manajemen konfigurasi keamanan yang kompleks, update sistem yang dapat mengganggu operasi kritis, dan keterbatasan bandwidth untuk transmisi data kesehatan yang berukuran besar (seperti image medis). Selain itu, terdapat tantangan dalam mengimplementasikan keamanan pada perangkat IoT medis (*Internet of Medical Things*) yang sering kali memiliki keterbatasan daya komputasi dan memori yang membuat implementasi enkripsi kuat menjadi sulit. Organisasi kesehatan juga menghadapi tantangan dalam merawat infrastruktur keamanan yang terus berkembang sambil menjaga uptime sistem yang tinggi, karena downtime dalam sistem kesehatan dapat berdampak langsung pada keselamatan pasien (Gowthamani et al., 2025).

10.4.2 Tantangan Organisasi dan Sumber Daya Manusia

Di luar tantangan teknis, terdapat tantangan organisasi yang signifikan dalam implementasi keamanan data kesehatan. Salah satu tantangan terbesar adalah keterbatasan anggaran dan sumber daya manusia. Banyak institusi kesehatan, terutama di negara berkembang, memiliki anggaran terbatas untuk investasi dalam infrastruktur keamanan. Mereka sering kali harus memprioritaskan pengeluaran untuk kebutuhan klinis langsung daripada investasi dalam keamanan teknologi informasi. Selain itu, terdapat kekurangan tenaga ahli keamanan siber yang memahami domain kesehatan secara spesifik, membuat rekrutmen dan retensi staf keamanan menjadi sulit.

Tantangan lainnya adalah perubahan budaya organisasi yang diperlukan untuk menciptakan kesadaran keamanan di seluruh tingkat organisasi. Staf kesehatan yang terlatih secara medis tetapi tidak memiliki latar belakang teknis sering kali tidak memahami pentingnya praktik keamanan, seperti membuat kata sandi yang kuat atau tidak membagikan kredensial. Pelatihan keamanan informasi harus disesuaikan dengan kebutuhan dan peran spesifik setiap staf, dan harus diulang secara berkala untuk memastikan bahwa kesadaran keamanan tetap terjaga. Manajemen perubahan juga menjadi tantangan ketika implementasi sistem keamanan baru dapat menambah beban kerja staf yang sudah sibuk (Riswaya & Wahyudi, 2025).

10.4.3 Strategi Implementasi Keamanan yang Efektif

Untuk mengatasi tantangan-tantangan tersebut, organisasi kesehatan harus mengadopsi strategi implementasi keamanan yang komprehensif dan terencana dengan baik. Pertama, organisasi harus melakukan *risk assessment* atau penilaian risiko yang menyeluruh untuk mengidentifikasi aset yang paling penting, ancaman yang paling mungkin, dan kerentanan yang ada dalam sistem mereka. Hasil dari penilaian risiko ini harus menjadi dasar untuk memprioritaskan investasi keamanan, fokus pada perlindungan aset yang paling bernilai dan risiko yang paling signifikan.

Kedua, organisasi harus mengembangkan kebijakan keamanan informasi yang jelas dan komprehensif yang mencakup semua aspek keamanan data, dari pembatasan akses hingga respons insiden. Kebijakan ini harus didokumentasikan dengan baik, dikomunikasikan kepada semua staf, dan ditegakkan secara konsisten. Ketiga, organisasi harus berinvestasi dalam teknologi keamanan yang sesuai dengan kebutuhan spesifik mereka, seperti enkripsi data, firewall, *intrusion detection systems*, dan *security information and event management* (SIEM). Namun, adopsi teknologi harus dikombinasikan dengan praktik terbaik organisasi dan pelatihan staf untuk memastikan efektivitas maksimal (Makinde, 2025).

Keempat, organisasi harus membangun kultur keamanan yang kuat di mana keamanan data dianggap sebagai tanggung jawab

bersama semua staf, bukan hanya tim keamanan. Ini memerlukan pelatihan keamanan reguler, kampanye kesadaran keamanan, dan penghargaan untuk perilaku keamanan yang baik. Kelima, organisasi harus memiliki rencana respons insiden yang jelas dan diuji secara berkala untuk memastikan bahwa mereka dapat merespons dengan cepat dan efektif jika terjadi pelanggaran keamanan. Rencana ini harus mencakup prosedur isolasi sistem yang terkena dampak, notifikasi pihak yang terkena, dan pelaporan kepada otoritas yang relevan.

10.4.4 Praktik Terbaik dalam Implementasi Keamanan Data

Terdapat sejumlah praktik terbaik yang telah terbukti efektif dalam mengimplementasikan keamanan data dalam layanan kesehatan. Salah satu praktik terbaik adalah *defense in depth* atau pertahanan berlapis, yang berarti mengimplementasikan kontrol keamanan di berbagai lapisan sistem sehingga jika satu lapisan dikompromikan, lapisan lainnya masih memberikan perlindungan. Ini dapat mencakup kombinasi enkripsi, kontrol akses, monitoring, dan mekanisme deteksi ancaman.

Praktik terbaik lainnya adalah *principle of least privilege*, di mana setiap pengguna diberikan hak akses minimum yang diperlukan untuk melakukan pekerjaan mereka. Ini mengurangi risiko bahwa kredensial yang dikompromikan dapat digunakan untuk mengakses data yang tidak relevan dengan pekerjaan pengguna tersebut. Selain itu, organisasi harus menerapkan *regular patching and updates* untuk semua sistem untuk memastikan bahwa

kerentanan yang diketahui diperbaiki dengan cepat. Dalam konteks kesehatan, ini harus dilakukan dengan hati-hati untuk menghindari mengganggu sistem kritis, sering kali memerlukan perencanaan yang matang dan komunikasi dengan staf klinis (Mathur et al., 2025).

Praktik terbaik lainnya adalah *encryption by default*, di mana semua data secara otomatis dienkripsi kecuali ada alasan spesifik untuk tidak melakukannya. Ini memastikan bahwa bahkan jika kontrol akses tergagal, data tetap terlindungi. Organisasi juga harus mengimplementasikan *data minimization*, yang berarti hanya mengumpulkan, menyimpan, dan memproses data yang benar-benar diperlukan untuk tujuan yang sah. Ini mengurangi risiko privasi dan memudahkan manajemen data. Terakhir, organisasi harus membangun program keamanan yang berkelanjutan dan responsif terhadap ancaman yang berkembang, yang mencakup monitoring, evaluasi, dan perbaikan terus-menerus (Shojaei et al., 2024).

Selain aspek teknis, keberhasilan implementasi keamanan data juga dipengaruhi oleh budaya keamanan (security awareness culture) di lingkungan organisasi. Pelatihan keamanan siber secara rutin bagi tenaga kesehatan dan staf administratif sangat penting untuk meningkatkan kesadaran terhadap ancaman seperti phishing, social engineering, dan malware. Banyak insiden keamanan terjadi akibat kesalahan manusia (human error), sehingga edukasi pengguna menjadi bagian integral dalam strategi keamanan informasi layanan kesehatan (Kruse et al., 2017).

Latihan Soal

1. Jelaskan bagaimana prinsip *confidentiality*, *integrity*, dan *availability* (CIA) diterapkan secara praktis dalam sistem manajemen catatan medis elektronik rumah sakit, dan berikan contoh spesifik tentang bagaimana masing-masing prinsip ini dapat dikompromikan serta langkah-langkah pencegahan yang diperlukan untuk melindunginya.
2. Bandingkan dan kontraskan implementasi keamanan data antara layanan kesehatan tradisional yang berbasis on-premise dengan layanan kesehatan modern yang berbasis cloud. Jelaskan keuntungan dan kerugian dari masing-masing pendekatan, serta strategi yang dapat digunakan untuk mengintegrasikan keduanya dalam model *hybrid cloud*.
3. Diskusikan tantangan-tantangan utama yang dihadapi oleh organisasi kesehatan di negara berkembang dalam mengimplementasikan keamanan data yang mematuhi standar internasional seperti HIPAA dan GDPR. Bagaimana organisasi dapat menyesuaikan standar-standar ini dengan keterbatasan sumber daya mereka tanpa mengorbankan perlindungan data pasien?
4. Analisis peran teknologi *Blockchain* dalam meningkatkan keamanan dan privasi data kesehatan. Jelaskan bagaimana *Blockchain* dapat mengatasi beberapa tantangan yang ada dalam sistem kesehatan saat ini, serta identifikasi potensi keterbatasan

dan tantangan implementasi *Blockchain* dalam konteks layanan kesehatan.

5. Kembangkan rencana komprehensif untuk merespons insiden keamanan data (*data breach*) di rumah sakit. Rencana ini harus mencakup langkah-langkah sebelum insiden terjadi, tindakan segera yang harus dilakukan setelah insiden terdeteksi, dan prosedur pemulihan serta pembelajaran dari insiden untuk mencegah terjadinya kembali di masa depan.

DAFTAR PUSTAKA

Belani, H., Perković, T., Šolić, P., Karin, Ž., & Jurcev Savicevic, A. (2025). Health data and information ownership: Cybersecurity, protection and privacy perspectives. *2025 24th International Conference on Software, Telecommunications and Computer Networks (SplitTech)*, 1-6. **https://doi.org/10.23919/SpliTech65624.2025.11091762**

Fauziah, Yuli. (2014). Tinjauan Keamanan Sistem Pada Teknologi Cloud Computing. Jurnal Informatika, 8(1), 870-883.

Ginavanee, A., & Prasanna, S. (2024). Improving healthcare data management in HL7-based EHR systems with the secure infrastructure of Google Cloud Platform. *2024 IEEE 3rd International Conference on Industrial Electronics for Computing and Communications Engineering (ICoICI)*, 1-8. **https://doi.org/10.1109/ICoICI62503.2024.10696524**

Gowthamani, R., Manoj, S. O., Sasi, K., & Rani, K. (2025). Empowering integrity and confidentiality in smart healthcare systems through effective edge cryptographic strategies. *Advances in Engineering Software*, 189, 103569. **https://doi.org/10.1080/00051144.2025.2569115**

Ikawati, F. R., & Haris, M. (2024). Challenges in implementing digital medical records in Indonesian hospitals: Perspectives on technology, regulation, and data security. *ICIStech*

Conference Proceedings, 4(2), 70-82. **https://doi.org/10.62951/icistech.v4i2.70**

Kemenkes RI. (2024). Keputusan Direktur Jenderal Pelayanan Kesehatan Nomor HK.02.02/D/47104/2024 tentang Instrumen Survei Akreditasi Rumah Sakit. Jakarta: Dirjen Pelayanan Kesehatan Kemenkes RI.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and health care : official journal of the European Society for Engineering and Medicine, 25(1), 1–10. **https://doi.org/10.3233/THC-161263**

Kumar, R., & Singh, M. (2023). Big data analytics and cloud computing applications in healthcare systems. *International Journal of Health Informatics*, 9(1), 33–41. **https://journal.uad.ac.id/index.php/JIFO/article/view/2087**

Latha, D. (2024). *Blockchain* solutions for secure healthcare data management: A comprehensive survey. *International Journal of Science and Research*, 29730, 1-12. **https://doi.org/10.55041/ijsrem29730**

Makinde, O. F. (2025). Navigating cyber threats in health information systems: Safeguarding patient and clinical data. *World Journal of Advanced Research and Reviews*,

28(1), 3566-3582. **https://doi.org/10.30574/wjarr.2025.28.1.3566**

Mathur, N., Seralathan, S., & Kalyanpur, A. (2025). Implementation of cybersecurity systems in teleradiology services- Best practices. *Medical Research Archives*, 13(2), 6237-6251. **https://doi.org/10.18103/mra.v13i2.6237**

Riswaya, A. R., & Wahyudi, H. (2025). Improving the efficiency of healthcare services in medical practices through a web-based data management system. *Bisnis dan Teknologi*, 18(2), 415-428. **https://doi.org/10.55208/bistek.v18i2.415**

Shojaei, P., VlahuGjorgievska, E., & Chow, Y.-W. (2024). Security and privacy of technologies in health information systems: A systematic literature review. *Computers*, 13(2), 41-58. **https://doi.org/10.3390/computers13020041**

Smith, D. A., & Abbasi, N. (2024). Cybersecurity in healthcare: Securing patient health information (PHI), HIPAA compliance framework and the responsibilities of healthcare providers. *Journal of Knowledge and Learning Science and Technology*, 3(3), 278-287. **https://doi.org/10.60087/jklst.vol3.n3.p.278-287**

PROFIL PENULIS

Nama : Sri Lestari, SKM, M. Kes

Tempat/tanggal lahir : Banyumas, 23 Februari 1966

Riwayat Pendidikan : SDN Kalisube Banyumas lulus 1979

- SMPN Banyumas lulus 1982
- SMAN Banyumas lulus 1985
- D3 APK-TS “HAKLI” lulus 1988
- S1 FKM UNDIP lulus 2001
- S2 Simkes UNDIP lulus 2009
- D3 RMIK lulus 2023

Pekerjaan : Dosen Jurusan RMIK Poltekkes Kemenkes Semarang

Pesan untuk pembaca : Membacalah, karena dengan banyak membaca melatih daya ingat dan mencegah pikun.

Nama : Indah Naryanti, SKM, MKM

Tempat/tanggal lahir : Semarang/3 Juni 1980

Riwayat Pendidikan :

- S1 Kesehatan Masyarakat Universitas Diponegoro Semarang
- S2 Kesehatan Masyarakat Universitas Diponegoro Semarang

Pekerjaan : Dosen

Pesan untuk pembaca : "Terima kasih kehadiran pembaca memberikan makna dalam setiap karya. Untaian kata yang ditorehkan, menambah pemahaman tentang Rekam Medis Elektronik dan sebagai komponen penting dalam transformasi digital pelayanan kesehatan."

Nama : Arief Azhari Ilyas, A.Md. RMIK., S.St., M.K.M

Tempat/tgl lahir : Rappang/ 22 Februari 1995

Alamat : Kota Semarang, Jawa Tengah.

Riwayat Pendidikan :

- Rekam Medis dan Informasi Kesehatan (D-III) STIKES Panakkukang Makassar (Lulus Tahun 2015).
- Manajemen Informasi Kesehatan (D-IV) Universitas Esa Unggul (Lulus Tahun 2017).
- Kesehatan Masyarakat (S-2) Universitas Hasanuddin (Lulus Tahun 2020).

Pekerjaan : Dosen

Pesan untuk pembaca : "Semoga buku ini dapat menjadi jembatan ilmu yang bermanfaat bagi para akademisi, praktisi, dan pemerhati keamanan data dalam memahami dan menerapkan

prinsip-prinsip perlindungan informasi di era digital, khususnya dalam konteks transformasi kesehatan di Indonesia."

Nama : Natalia Kristiani, A.Md., S.KM, M.K.M

Tempat/tanggal lahir : Wonogiri, 28 Desember 1982

Riwayat Pendidikan : Magister Kesehatan Masyarakat Universitas Diponegoro Semarang

- S1 Kesehatan Masyarakat STIKES HAKLI Semarang
- D3 Rekam Medis Universitas AKI Semarang

Pekerjaan : Medical Record RS Khusus Bedah Columbia Asia Semarang

Pesan untuk pembaca : Semoga isi buku ini dapat memberikan wawasan, pengetahuan, serta kesadaran bagi tenaga kesehatan, pengelola rekam medis, dan seluruh pihak terkait dalam menghadapi berbagai risiko dan ancaman terhadap keamanan data di fasilitas kesehatan.

Nama : Setya Wijayanta, S.T., M.Kes

Tempat/tanggal lahir : Gunungkidul, 17 Desember 1985

Riwayat Pendidikan : Magister Ilmu Kesehatan Masyarakat

Pekerjaan : Dosen

Pesan untuk pembaca : "Keamanan data kesehatan bukan hanya persoalan regulasi, tetapi wujud nyata kepercayaan yang diberikan pasien kepada kita. Buku ini hadir untuk membangun kesadaran dan kompetensi, agar dosen, mahasiswa, serta pengelola fasilitas pelayanan kesehatan mampu menjalankan tanggung jawab perlindungan data secara profesional dan berkelanjutan. Sudah saatnya keamanan informasi kesehatan menjadi budaya kerja, bukan sekadar kewajiban administratif."

Nama : Praditya Dewi Arumsari, S.E., M.Si

Tempat/tanggal lahir : Banda Aceh/ 5 Agustus 1991

Alamat : Banyumanik, Kota Semarang

Riwayat Pendidikan :

- Sarjana Akuntansi Universitas Muhammadiyah Semarang
- Magister Akuntansi Universitas Diponegoro

Pekerjaan : Dosen Jurusan Rekam Medis dan Informasi Kesehatan Poltekkes Kemenkes Semarang

Pesan untuk pembaca : -

Nama : Dyah Ayu Puspitaningtyas, M.Tr.ID

Tempat/tanggal lahir : Ngawi, 24 April 1994

Riwayat Pendidikan : Magister Terapan Imaging Diagnostik, Poltekkes Semarang

Pekerjaan : Dosen

pesan untuk pembaca : Semoga buku "Patofisiologi: Dasar Klinis untuk Radiologi" bermanfaat untuk semua pembaca, baik dari kalangan mahasiswa, profesi tenaga kesehatan ataupun umum. Dengan adanya buku ini diharapkan bisa menjadi rujukan ataupun referensi untuk pembelajaran.

Nama : Rudiansyah, SKM., M. Kes

Tempat/Tanggal Lahir : Tain, 08 September 1988

Kota Domisili : Sintang, Kalimantan Barat

Hobi : Baca Buku, Traveling dan Menulis

Pesan untuk pembaca : Ilmu adalah amanah, dan menulis adalah salah satu cara menunaikan amanah itu. Semoga buku ini menjadi ladang amal jariyah, dan semoga pembaca mendapatkan manfaat serta inspirasi untuk terus berkontribusi di jalan ilmu dan kebaikan.

Nama : Edi Sugiarto, SKM., M.Kes

Tempat/Tanggal Lahir : Waimital, 08 Mei 1985

Riwayat Pendidikan :

- S1 Kesehatan Mayarakat STIKes Maluku Husada peminatan Epidemiologi.
- S2 Kesehatan Masyarakat Universitas Airlangga Surabaya peminatan Biostatistika.

Pengalaman : Sebagai Analis data kesehatan di beberapa Fasilitas pelayanan kesehatan di tingkat Kabupaten. Sebagai Penulis buku

Pekerjaan : Dosen tetap di Program Studi Kesehatanmasyarakat STIKes Maluku Husada

Pesan untuk pembaca : “Teruslah belajar sampai engkau dapat menaklukkan Dunia”.

Nama : Muhammad Rifqi Aufa Daffa, A.Md.Kes

Tempat/tanggal lahir : Brebes, 08 Maret 2001

Riwayat Pendidikan : D3 Rekam Medis dan Informasi Kesehatan

Pekerjaan : Tenaga Kependidikan

Pesan untuk pembaca : Tetaplah menulis dan menginspirasi, seperti kopi yang selalu mendampingi dan menginspirasi untuk mengisi kosongnya hati dan pikiran.

Buku ***Keamanan dan Kerahasiaan Data dalam Sistem Kesehatan*** membahas pentingnya perlindungan informasi kesehatan di era digital yang semakin berkembang. Pengelolaan data kesehatan yang aman dan terpercaya menjadi salah satu aspek penting dalam menjaga privasi individu, meningkatkan kualitas pelayanan, serta membangun kepercayaan masyarakat terhadap sistem kesehatan.

Disusun dengan bahasa yang mudah dipahami, buku ini mengulas berbagai aspek keamanan informasi kesehatan, perlindungan data pribadi, pengelolaan rekam medis elektronik, ancaman keamanan siber, serta langkah-langkah yang dapat diterapkan untuk menjaga kerahasiaan dan integritas data. Pembahasan juga menyoroti peran teknologi dan tanggung jawab berbagai pihak dalam memastikan keamanan informasi kesehatan.

Buku ini sangat cocok untuk masyarakat umum yang ingin memahami pentingnya menjaga keamanan dan kerahasiaan data kesehatan di tengah pesatnya perkembangan teknologi informasi. Dengan wawasan yang praktis dan informatif, buku ini membantu pembaca lebih sadar akan pentingnya perlindungan data pribadi sebagai bagian dari upaya menciptakan layanan kesehatan yang aman, terpercaya, dan berkelanjutan.

selat media

ISBN 978-634-7465-83-2 (PDF)