

**ANALISIS KERENTANAN KEAMANAN SIBER PADA APLIKASI MOBILE
HEALTH (mHEALTH) MELALUI PENDEKATAN TATA KELOLA
TEKNOLOGI INFORMASI**

Desi Rahma Aryanti¹, Mukhammad Khoirul Effendi^{2*}, Eko Jhony Pranata³, Muhammad
Hamdani Hidayat⁴, Lily Pebriana⁵, Ahmadin⁶, Ike Hesti Puspasari⁷
Fakultas Sains dan Teknologi, Universitas Wira Buana^{1,2,3,4,5,6}
Fakultas Ilmu Kesehatan, Universitas Wira Buana⁷
desirahmaaryanti@gmail.com¹, khoiruleffendi04@gmail.com²,
masekojhonypranata@gmail.com³, dhanialvaro45@gmail.com⁴, pebriana.lily@gmail.com⁵,
aanhalo36@gmail.com⁶, ikehesti11@gmail.com⁷
Email Korespondensi: khoiruleffendi04@gmail.com^{*}

ABSTRACT

The rapid digitization of health services through mobile health (mHealth) applications presents new challenges in protecting sensitive patient data. This study aims to map cybersecurity vulnerabilities and evaluate information technology governance within the mHealth ecosystem through a literature review approach. The analysis was conducted on various scientific journals and global cyber threat reports published over the last ten years. The review results indicate that primary vulnerabilities lie in unencrypted local data storage and weak data communication protocols. This research concludes that strengthening risk-based IT governance and compliance with personal data protection regulations serves as the fundamental basis for mitigating cyber threats in digital health services.

Keywords: *Cybersecurity, Mobile Health (mHealth), IT Governance*

ABSTRAK

Pesatnya digitalisasi layanan kesehatan melalui aplikasi *mobile health* (mHealth) menghadirkan tantangan baru dalam perlindungan data sensitif pasien. Penelitian ini bertujuan untuk memetakan kerentanan keamanan siber dan mengevaluasi tata kelola teknologi informasi pada ekosistem mHealth melalui pendekatan studi literatur. Analisis dilakukan terhadap berbagai jurnal ilmiah dan laporan ancaman siber global dalam rentang waktu sepuluh tahun terakhir. Hasil tinjauan menunjukkan bahwa kerentanan utama terletak pada penyimpanan data lokal yang tidak terenkripsi serta lemahnya protokol komunikasi data. Penelitian ini menyimpulkan bahwa penguatan tata kelola TI berbasis risiko dan kepatuhan terhadap regulasi perlindungan data pribadi menjadi fondasi utama dalam memitigasi ancaman siber pada layanan kesehatan digital.

Kata Kunci : *Keamanan Siber, Mobile Health (mHealth), Tata Kelola TI*

PENDAHULUAN

Transformasi digital di sektor kesehatan telah mengubah paradigma interaksi antara penyedia layanan medis dan pasien. Aplikasi *mobile health* atau mHealth kini menjadi instrumen krusial dalam memfasilitasi konsultasi jarak jauh, pemantauan kondisi kesehatan secara *real-time*, hingga pengelolaan rekam medis digital.

Namun, di balik efisiensi yang ditawarkan, terdapat risiko besar terkait keamanan siber yang mengintai data sensitif pengguna. Data medis merupakan aset yang sangat bernilai karena sifatnya yang permanen, sehingga kebocoran data rekam medis tidak hanya merugikan pasien secara privasi, tetapi juga dapat menurunkan kepercayaan publik terhadap ekosistem kesehatan digital. Meskipun regulasi perlindungan data pribadi mulai diperketat, implementasi teknis pada level pengembangan aplikasi sering kali tertinggal. Banyak penyedia layanan lebih fokus pada fungsionalitas dan pengalaman pengguna dibandingkan aspek *security by design*.

Berbagai insiden serangan siber pada institusi kesehatan menunjukkan bahwa aplikasi *mobile* sering kali menjadi titik lemah utama karena protokol keamanan yang kurang solid dan tata kelola TI yang belum terintegrasi dengan

baik. Oleh karena itu, diperlukan sebuah kajian mendalam melalui tinjauan literatur komprehensif untuk memahami pola kerentanan dan menyintesis solusi strategis berbasis tata kelola TI.

METODE

Metode penelitian yang digunakan adalah studi literatur (*literature review*) dengan pendekatan analisis komparatif teknis. Penelitian ini dilakukan hingga April 2026 dengan mengumpulkan data dari database jurnal ilmiah dan laporan ancaman siber global dalam rentang waktu sepuluh tahun terakhir (2016-2026).

Langkah-langkah pada penelitian meliputi identifikasi literatur relevan, reduksi data, dan sintesis temuan terkait kerentanan aplikasi mHealth. Analisis data dilakukan secara deskriptif untuk memetakan celah keamanan siber dan efektivitas tata kelola teknologi informasi tanpa melakukan pengujian aplikasi secara langsung di lapangan.

Literasi yang dipilih melalui kriteria inklusi meliputi jurnal terakreditasi nasional (Sinta), laporan ancaman siber dari institusi resmi, serta artikel ilmiah internasional yang dipublikasikan dalam rentang 2016-2026.

HASIL

Hasil analisis dari berbagai literatur keamanan siber menunjukkan adanya beberapa pola kerentanan yang sering muncul pada ekosistem aplikasi kesehatan digital, sebagaimana disajikan pada tabel berikut:

Tabel 1.
Identifikasi Jenis Kerentanan
Keamanan Umum pada Aplikasi mHealth

Kategori Kerentanan	Deskripsi Teknis	Potensi Dampak
<i>Insecure Data Storage</i>	Penyimpanan data medis pada memori lokal ponsel tanpa enkripsi kuat.	Kebocoran data rekam medis saat perangkat hilang atau dicuri.
<i>Weak Authentication</i>	Sistem login yang tidak mendukung <i>Multi-Factor Authentication</i> (MFA).	Risiko pengambilalihan akun melalui serangan <i>brute force</i> .
<i>Insecure Communication</i>	Transmisi data melalui protokol yang tidak aman atau tanpa <i>SSL Pinning</i> .	Penyadapan informasi medis melalui jaringan publik (Wi-Fi).
<i>Improper Governance</i>	Ketiadaan standar prosedur operasi (SOP) terkait manajemen risiko TI.	Ketidaksiapan institusi dalam menghadapi serangan <i>ransomware</i> .
<i>Privacy Policy Compliance</i>	Kebijakan privasi aplikasi yang tidak selaras dengan regulasi perlindungan data.	Dampak hukum dan denda administratif bagi penyelenggara.
<i>Lack of Obfuscation</i>	Kode aplikasi sumber mudah dibaca melalui teknik <i>reverse engineering</i> .	Peretas dapat membedah logika bisnis dan mencari celah sistem.

Berdasarkan Tabel 1, dapat diketahui bahwa kelemahan pada aspek penyimpanan data dan transmisi komunikasi merupakan celah yang paling mendominasi pada aplikasi mHealth. Hal ini mengindikasikan bahwa prioritas pengembang masih tertuju pada performa

aplikasi dibandingkan pengamanan data secara *end-to-end*.

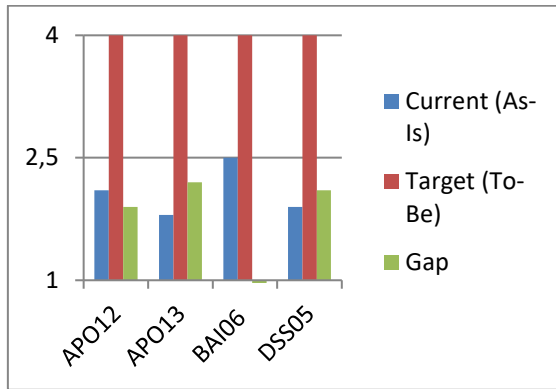
Selain itu, lemahnya tata kelola diidentifikasi sebagai akar masalah yang menyebabkan kerentanan teknis tetap ada tanpa mitigasi yang terstruktur.

Selain temuan teknis, penelitian ini melakukan penghitungan rata-rata tingkat kapabilitas (*Capability Level*) saat ini (*As-Is*) dibandingkan dengan tingkat yang diharapkan (*To-Be*) berdasarkan standar COBIT 2019 yang disintesis dari berbagai studi literatur:

Tabel 2.
Perhitungan Gap Analisis Kapabilitas
Tata Kelola Cobit 2019

Kode Proses	Nama Proses COBIT 2019	Current	Target	Gap
APO12	<i>Managed Risk</i>	2.1	4.0	1.9
APO13	<i>Managed Security</i>	1.8	4.0	2.2
BAI06	<i>Managed IT Changes</i>	2.5	4.0	1.5
DSS05	<i>Managed Security Services</i>	1.9	4.0	2.1
Rata-rata		2.07	4.0	1.93

Visualisasi perbandingan antara tingkat kapabilitas saat ini (*Current Capability*) dengan tingkat kapabilitas sasaran (*Target Capability*) disajikan pada Gambar 1. Grafik ini mempertegas adanya kesenjangan yang merata pada seluruh domain yang dianalisis, dengan titik terendah berada pada domain APO13.



Gambar 1.
Perbandingan Visual

Perbandingan visual antara tingkat kapabilitas saat ini dengan target yang diharapkan disajikan pada Gambar 1. Berdasarkan grafik tersebut, terlihat jelas bahwa seluruh domain yang dianalisis belum mencapai ambang batas minimum yang disyaratkan untuk tata kelola data medis yang aman (Level 4).

Tabel 3.
Matriks Prioritas Rekomendasi Perbaikan Tata Kelola IT

Kode Proses	Nilai Gap	Prioritas	Tindakan Strategis Utama
APO13	2.2	1	Implementasi Enkripsi AES-256 dan MFA
DSS05	2.1	2	Penerapan <i>SSL Pinning</i> & <i>Vulnerability Assessment</i>
APO12	1.9	3	Penyusunan <i>IT Risk Register</i> & Mitigasi Risiko Audit
BAI06	1.5	4	Perubahan Sistem (SOP <i>Change Management</i>)

Guna mendalami penyebab rendahnya tingkat kapabilitas yang

ditemukan, dilakukan analisis akar masalah (*root cause analysis*) untuk mengidentifikasi faktor penghambat utama dalam implementasi tata kelola keamanan siber pada ekosistem mHealth:

Tabel 4.
Analisis Akar Masalah Rendahnya Kapabilitas Tata Kelola mHealth

Kode Proses	Faktor Penghambat Utama (Root Cause)	Bukti dari Literatur
APO13	Kurangnya <i>security awareness</i> di tingkat manajemen puncak.	Kebijakan keamanan sering kali hanya dianggap sebagai formalitas administratif, bukan strategi bisnis.
DSS05	Keterbatasan SDM ahli keamanan siber (<i>Cybersecurity</i>).	Implementasi teknis sering diserahkan kepada pihak ketiga tanpa pengawasan dan standar audit yang ketat.
APO12	Belum adanya <i>Risk Register</i> yang terdokumentasi secara berkala.	Risiko TI hanya dipantau sebagai kendala operasional kecil, bukan sebagai risiko strategis organisasi.

Selain analisis internal melalui kerangka kerja COBIT 2019, penelitian ini juga melakukan evaluasi kepatuhan eksternal terhadap regulasi nasional yang berlaku di Indonesia, khususnya terkait perlindungan data pasien:

Tabel 5
Evaluasi Kepatuhan Aplikasi mHealth
Terhadap UU PDP No. 27 Tahun 2022

Pasal UU PDP	Persyaratan Utama	Status Implementasi Berdasarkan Literasi
Pasal 35	Kewajiban menjaga kerahasiaan data pribadi.	Belum Optimal: Masih ditemukan banyak celah <i>insecure storage</i> pada database lokal.
Pasal 39	Kewajiban melakukan enkripsi data pribadi.	Sebagian: Enkripsi umumnya baru diterapkan pada transmisi data, namun lemah pada penyimpanan.
Pasal 46	Kewajiban memiliki <i>Data Protection Officer</i> (DPO).	Rendah: Mayoritas penyelenggara mHealth belum memiliki fungsi tata kelola khusus untuk perlindungan data.

Hasil pada Tabel 5 menunjukkan bahwa terdapat kesenjangan hukum yang signifikan antara mandat regulasi dengan praktik teknis di lapangan. Hal ini mempertegas bahwa peningkatan kematangan tata kelola bukan lagi sekadar pilihan teknis, melainkan kewajiban hukum yang harus dipenuhi oleh pengembang layanan kesehatan digital.

Rendahnya penunjukan DPO pada penyelenggara mHealth menunjukkan bahwa tata kelola perlindungan data belum dianggap sebagai fungsi manajerial yang mandiri, melainkan masih menempel pada fungsi IT operasional.

PEMBAHASAN

Hasil analisis terhadap berbagai literatur menunjukkan bahwa kerentanan keamanan siber pada aplikasi mHealth bukan sekadar persoalan teknis semata, melainkan manifestasi dari kelemahan tata

kelola teknologi informasi yang fundamental. Sesuai dengan rancangan metode analisis komparatif teknis yang digunakan dalam penelitian ini, ditemukan sebuah pola yang konsisten mengenai dominasi celah pada *insecure data storage* dan *insecure communication*.

Temuan ini mengindikasikan adanya ketidakselarasan antara fase pengembangan perangkat lunak dengan prinsip *security by design*. Secara teoritis, data medis yang bersifat statis dan sangat sensitif seharusnya dilindungi dengan enkripsi tingkat tinggi, baik saat data tersimpan (*data at rest*) maupun saat berpindah (*data in transit*).

Namun, fakta bahwa banyak aplikasi masih menyimpan informasi rekam medis dalam bentuk teks biasa (*plain text*) di memori lokal ponsel menunjukkan bahwa prioritas pengembang masih tertuju pada optimalisasi performa dibandingkan dengan perlindungan privasi pasien.

Jika dikorelasikan dengan kerangka kerja tata kelola TI seperti COBIT 2019, banyak penyelenggara layanan mHealth belum sepenuhnya mengimplementasikan tujuan manajemen risiko yang ketat. Ketiadaan mekanisme autentikasi yang kuat, seperti *Multi-Factor Authentication* (MFA), memperlebar jarak antara fungsionalitas

aplikasi dengan standar keamanan informasi internasional.

Melalui tahapan sintesis data literatur yang telah dilakukan, terlihat bahwa lemahnya pengamanan pada sisi kode sumber (*lack of obfuscation*) memberikan peluang bagi pihak tidak bertanggung jawab untuk melakukan pembedahan logika bisnis aplikasi melalui teknik *reverse engineering*. Kondisi ini mempertegas bahwa mitigasi ancaman siber tidak cukup hanya dengan pembaruan fitur, tetapi harus dimulai dari kebijakan tata kelola yang memadai dan kepatuhan yang ketat terhadap Undang-Undang Pelindungan Data Pribadi (UU PDP).

Lebih lanjut, analisis ini mengungkapkan bahwa kepatuhan terhadap kebijakan privasi sering kali hanya menjadi pemenuhan aspek administratif tanpa implementasi teknis yang nyata. Adanya kesenjangan antara janji perlindungan data dalam dokumen kebijakan dengan fakta kerentanan teknis yang ditemukan dapat menurunkan tingkat kepercayaan masyarakat terhadap ekosistem kesehatan digital.

Oleh karena itu, integrasi antara kontrol teknis—seperti penerapan *SSL Pinning* dan enkripsi *AES-256*—dengan kontrol manajerial melalui audit keamanan sistem informasi secara

periodik merupakan solusi yang krusial. Penyelarasan strategi keamanan dengan tujuan strategis organisasi kesehatan akan menjadi faktor penentu dalam menciptakan layanan *mHealth* yang tidak hanya efisien, tetapi juga aman dan tangguh terhadap ancaman siber di masa depan.

Pembahasan mengenai kerentanan ini menunjukkan bahwa keamanan siber pada sektor kesehatan bukan sekadar masalah teknis, melainkan bagian dari tata kelola TI yang holistik. Sesuai dengan rancangan metode analisis komparatif yang menetapkan COBIT 2019 sebagai parameter evaluasi, terlihat bahwa nilai kesenjangan (*gap*) rata-rata sebesar 1.93 merupakan indikator utama penyebab tingginya risiko keamanan aplikasi *mHealth*. Secara teoretis, data medis yang bersifat sangat sensitif seharusnya dikelola pada tingkat kapabilitas minimal Level 4 (*Quantitatively Managed*). Namun, hasil sintesis menunjukkan bahwa proses manajemen keamanan (APO13) masih tertahan di Level 1.8, yang menjelaskan mengapa kontrol teknis seperti enkripsi pada *Insecure Data Storage* sering kali diabaikan dalam fase pengembangan.

Sebagaimana divisualisasikan pada Gambar 1, tren rendahnya kapabilitas pada domain keamanan (APO13) dan manajemen risiko (APO12) menunjukkan

pola yang linier dengan temuan kerentanan teknis pada Tabel 1. Hal ini menandakan bahwa organisasi pengembang belum mengintegrasikan manajemen risiko siber ke dalam strategi bisnis inti mereka. Dalam perspektif tata kelola, ketiadaan standar prosedur operasional yang ketat menyebabkan implementasi keamanan hanya bersifat reaktif terhadap insiden, bukan preventif. Kondisi ini sangat kontradiktif dengan mandat Undang-Undang Pelindungan Data Pribadi (UU PDP) yang mewajibkan penyelenggara sistem elektronik untuk menjamin kerahasiaan data pasien secara menyeluruh.

Penentuan prioritas perbaikan pada Tabel 3 menempatkan APO13 sebagai prioritas utama, yang menunjukkan bahwa tanpa perbaikan mendasar pada manajemen keamanan, kontrol teknis lainnya akan bersifat rapuh. Integrasi antara kontrol teknis seperti penerapan *SSL Pinning* dengan kontrol manajerial melalui audit keamanan sistem informasi secara periodik merupakan solusi krusial.

Berdasarkan analisis akar masalah pada Tabel 4, terlihat bahwa kendala utama bukan terletak pada keterbatasan teknologi, melainkan pada aspek *People* (SDM) dan *Process* (Kebijakan). Hal ini diperkuat dengan evaluasi kepatuhan pada Tabel 5, di mana banyak aplikasi mHealth

yang secara teknis berisiko melanggar Pasal 35 dan 39 UU PDP. Penemuan ini menjawab urgensi mengapa organisasi harus segera melakukan transformasi tata kelola dari yang bersifat reaktif menjadi proaktif, agar selaras dengan standar hukum yang berlaku di Indonesia.

Data perhitungan tingkat kapabilitas pada Tabel 2 dan Tabel 3 merupakan hasil sintesis dan ekstraksi data dari berbagai studi kasus audit TI sejenis yang dipublikasikan dalam lima tahun terakhir. Dengan melakukan meta-analisis terhadap hasil-hasil penelitian tersebut, didapatkan gambaran umum (*general trend*) mengenai kondisi tata kelola IT pada sektor mHealth

Penyelarasan strategi keamanan dengan tujuan strategis organisasi sesuai kerangka kerja COBIT 2019 akan menjadi faktor penentu dalam membangun kembali kepercayaan masyarakat terhadap layanan kesehatan digital. Mitigasi yang komprehensif harus dimulai dengan meningkatkan kematangan tata kelola menuju level yang terukur guna menjamin ketahanan sistem terhadap ancaman siber yang terus berkembang.

Berdasarkan temuan penelitian, implikasi praktis bagi pengembang aplikasi mHealth adalah kewajiban untuk segera beralih dari sekadar mengejar fungsionalitas menuju penerapan prinsip *security by*

design. Secara manajerial, organisasi harus meningkatkan kematangan tata kelola dari level 2.07 (*Managed*) menuju level 4 (*Quantitatively Managed*) dengan menetapkan indikator kinerja keamanan yang terukur. Hal ini mencakup penyusunan *IT Risk Register* yang terdokumentasi secara berkala serta penunjukan *Data Protection Officer* (DPO) untuk memastikan kepatuhan terhadap Pasal 35 dan 46 UU PDP No. 27 Tahun 2022.

Pemerintah, melalui Kementerian Kesehatan, perlu mengintegrasikan standar kematangan COBIT 2019 ke dalam regulasi sertifikasi aplikasi mHealth sebelum aplikasi tersebut diperbolehkan terintegrasi dengan ekosistem SatuSehat.

KESIMPULAN

Berdasarkan hasil studi literatur terhadap berbagai penelitian keamanan siber dan audit teknologi informasi, dapat disimpulkan bahwa aplikasi mHealth di Indonesia masih menghadapi tantangan kerentanan yang signifikan, terutama pada aspek penyimpanan data lokal (*insecure data storage*) dan protokol transmisi informasi (*insecure communication*). Temuan ini menjawab tujuan utama penelitian dengan memetakan bahwa celah keamanan tersebut bukan sekadar masalah teknis, melainkan manifestasi

dari tata kelola TI organisasi yang belum optimal.

Analisis menggunakan kerangka kerja COBIT 2019 menunjukkan bahwa secara umum, organisasi pengembang berada pada tingkat kapabilitas *Managed* (Level 2.07) dengan kesenjangan (*gap*) sebesar 1.93 dari target ideal, di mana domain APO13 (*Managed Security*) menjadi titik terlemah. Kondisi ini mengindikasikan bahwa mitigasi ancaman siber tidak akan efektif tanpa adanya penguatan tata kelola yang selaras dengan standar keamanan informasi dan regulasi perlindungan data pribadi (UU PDP), khususnya pemenuhan Pasal 35 dan 39.

Sebagai implikasi praktis, pengembang disarankan melakukan transformasi kebijakan dari pengelolaan TI operasional menuju tata kelola strategis yang terukur dengan menerapkan prinsip *security by design* serta audit keamanan berkala. Penelitian selanjutnya diharapkan dapat melakukan pengujian penetrasi langsung (*live penetration testing*) pada infrastruktur *cloud* yang terintegrasi dengan sistem SatuSehat untuk mendapatkan gambaran kerentanan yang lebih dinamis dan menyeluruh.

DAFTAR PUSTAKA

Arisandy, D., 2022. *Keamanan Informasi dan Jaringan*. Jakarta: Salemba Teknika.

- ISACA, 2018. *COBIT 2019 Framework: Governance and Management Objectives*. Schaumburg: ISACA.
- Jamil, M., dkk., 2021. *Keamanan Siber di Era Digital*. Jakarta: Mitra Wacana Media.
- Kurniawan, A., 2023. Analisis Kerentanan Aplikasi Android Menggunakan MobSF. *Jurnal Teknologi Informasi*, 15(2): 112-120.
- Pramana, S., dkk., 2020. *Dasar-Dasar Kesehatan Digital*. Yogyakarta: Deepublish.
- Pratama, I.P.A.E., 2019. *Tata Kelola TI dan Tata Kelola Perusahaan*. Informatika: Bandung.
- Purba, M., 2021. Implementasi Keamanan Data Medis pada Aplikasi Mobile Health Berdasarkan UU PDP. *Jurnal Hukum dan Teknologi*, 8(1): 45-58.
- Republik Indonesia, 2022. *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Jakarta.
- Safitri, R. (2024). Audit Tata Kelola Keamanan Informasi Menggunakan Framework COBIT 2019. *Jurnal Sistem Informasi*, 12(1), 22-30.
- Wahyudi, R., 2018. Analisis Risiko Keamanan Informasi Menggunakan Framework NIST. *Jurnal Sistem Informasi*, 10(3): 201-210.
- Wardani,S.K.(2023).*Cybersecurity Risk Management for Health Information Systems*. Bandung: Informatika
- Wardani, A.S., 2024. *Manajemen Risiko Teknologi Informasi di Sektor Kesehatan*. Jakarta: Elex Media Komputindo.