Sanskara Manajemen dan Bisnis
Vol. 02, No. 01, November, pp. 59-66
ISSN: 2963-024X, DOI: 10.58812/smb.v2i01

Analisis Keamanan Data *Electronic Medical Record Digital Transformation Office (DTO)* Kementerian Kesehatan Indonesia

Fitri Indriyajati[1], Maria Margarith Stely Damiana Jawa[2], Hargo Utomo[3]
[1] Universitas Gadjah Mada, fitri.indriyajati@mail.ugm.ac.id
[2] Universitas Gadjah Mada, mariamargarith99@mail.ugm.ac.id
[3] Universitas Gadjah Mada, hargo_utomo@ugm.ac.id

Article Info

Article history:

Received Jun 20, 2023
Revised Nov 17, 2023
Accepted Nov 28, 2023

Kata Kunci:

Digital Transformation Office, Kementerian Kesehatan Indonesia, Kesehatan Elektronik, Medis Elektronik, Perlindungan Data

Keywords:

Digital Transformation Office, Ministry of Health Indonesia, Electronic Health, Electronic Medical, Data Protection

ABSTRAK

Tata Pamong diperlukan untuk mengatur kebijakan regulasi dalam satu sistem data di Kementerian Kesehatan, terutama dengan adanya *big data* untuk Data Rekam Medis Elektronik yang terintegrasi yang akan digunakan untuk menganalisis data Kesehatan masyarakat Indonesia. Untuk mencapai hal ini, diperlukan keamanan data yang akan menjaga setiap data yang dibutuhkan sehingga konsep data terpadu dapat terwujud. Studi ini bertujuan untuk merekomendasikan spesifik keamanan data untuk data *microservice* di Digital *Transformation Office* Kementerian Kesehatan Indonesia. Metode penelitian adalah dengan menganalisis dokumen berupa Cetak Biru Rencana Strategi Transformasi Digital Kesehatan Tahun 2024 dan Laporan Tahunan Tahun 2022 dari Situs Web Kementerian Kesehatan. Data yang digunakan adalah data sekunder. Dengan perkembangan teknologi, Kementerian Kesehatan dapat melindungi keamanan data pasien melalui beberapa Langkah yaitu *autentikasi*, kontrol akses dan enkripsi.

ABSTRACT

The corporate government needed to regulate the regulation of policies in a single data system at the Indonesian Ministry of Health. Especially with the existence of big data for the Integrated Electronic Health Record which will be used to analyze health data for all people in Indonesia. To achieve this, data security is needed which will guard every data needed so that the concept of one integrated data will be realized. This paper aims to recommend data security specifications for microservice data in the Digital Transformation Office (DTO) of the Indonesian Ministry of Health. The research method is to analyze documents in the form of the 2024 Health Digital Transformation Strategy Blueprint and the 2022th Annual Report. With today's developing technology, it will help the Ministry of Health protect the security of sensitive patient data in several stages, namely authentication, access control and encryption.

Corresponding Author:

Name: Fitri Indriyajati
Institution: FEB UGM Jalan Sosio Humaniora No.1 Bulaksumur Depok Sleman Yogyakarta 55281
Email: fitri.indriyajati@mail.ugm.ac.id

1. PENDAHULUAN

Sistem pemantauan kesehatan menunjukkan sistem terkait dengan pengumpulan, analisis, dan interpretasi sistematis terkait data kesehatan untuk tujuan pengawasan dan mendeteksi perubahan status kesehatan didalam masyarakat. Sistem ini memainkan peran penting dalam kesehatan publik yang menyediakan informasi secara waktu dan akurat yang dapat digunakan untuk mencegah penyakit, merespons adanya wabah dan pengembangan kebijakan. Peraturan Menteri Kesehatan Republik Indonesia Nomor 12 Tahun 2020 telah mewajibkan perubahan dalam pengaturan pengembangan sistem kesehatan yang mencakup integrasi *platform Indonesia Health Service* untuk sistem informasi, penelitian, dan pengembangan kesehatan dalam rentang waktu 2020-2024. *Platform Indonesia Health Service* memberikan hasil yang bermanfaat bagi seluruh ekosistem industri kesehatan yang terlibat di dalamnya. Hal ini meliputi data hasil analisis data dan informasi yang terintegrasi. *Platform Indonesia Health Service* mengintegrasikan data untuk mendukung fasilitas kesehatan dalam memberikan pelayanan yang optimal, terutama dalam hal memprediksi penyakit pada pasien. Peluang utama dari penggunaan data kesehatan adalah peningkatan kualitas layanan, manajemen kesehatan, deteksi dini penyakit, kualitas data, struktur dan aksesibilitas, pengembalian keputusan yang lebih baik, serta pengurangan biaya (Kruse et al., 2016).

Integrasi sistem dan pengembangan satu data rekam medis memerlukan tata pamong yang baik dalam mengatur kebijakan satu data tersebut. Adanya sistem satu data kesehatan terkait dengan individu (*integrated electronic health record)* di kementerian kesehatan akan membentuk big data yang perlu dianalisis untuk keperluan prediktif analisis kesehatan masyarakat Indonesia. Big data di industri kesehatan lebih kompleks dengan sifat *value, volume, velocity, veracity, variety, validity, viability, volatility, vulnerability dan visualization* (Gupta et al., 2023). Big data dan penggunaan analitis lanjutan memiliki potensi pengguna memanfaatkan teknologi tersebut untuk membuat keputusan klinis berdasarkan informasi tersebut (Kruse et al., 2016). Penggunaan big data di dalam industri kesehatan akan meningkatkan pelayanan untuk pengguna, membuat organisasi lebih fleksibel, meningkatkan kualitas, mengurangi biaya, mendukung proses pembuatan keputusan dan meningkatkan aktivitas pemantauan (Fanelli et al., 2023). Big data dan penggunaan analitik canggih memiliki potensi untuk memajukan cara penyedia memanfaatkan teknologi untuk membuat keputusan klinis berdasarkan informasi (Kruse et al., 2016). Akan tetapi, jumlah informasi besar tiap tahun yang dihasilkan dalam perawatan kesehatan harus diatur dan dikotak - kotakkan untuk memungkinkan aksesibilitas universal dan transparansi antara organisasi kesehatan. Fokus utama dalam sistem data kesehatan yang terintegrasi adalah tata pamong data kesehatan dan keamanan data yang diperlukan untuk mengamankan data kesehatan masyarakat.

Tantangan utama analisis data dalam industri kesehatan adalah struktur data, keamanan, standardisasi data, penyimpanan dan transfer, manajerial keterampilan seperti tata pamong data (Kruse et al., 2016). Tata kelola data bukanlah hal baru, hal yang perlu dipertanyakan terkait dengan siapa yang akan mengelola data kesehatan tersebut? dan bagaimana peran tata pamong tersebut dalam hal privasi dan keamanan (European Commission, 2020). Resiko adanya pelanggaran data dan identifikasi pasien tidak akan pernah sepenuhnya dihilangkan, akan tetapi biaya yang ditimbulkan karena tidak berbagi data akan lebih besar dan akan menghambat kemajuan Kesehatan(Holly et al., 2023). Di era digital ini tidak ada yang aman, penyerang dapat mencuri data kesehatan berbasis *B2B* yang disimpan di *server cloud* untuk memodifikasi data untuk keuntungan pribadi (Gupta et al., 2023).

Arus informasi digital dalam *Indonesia Health Service (IHS)* yang saling terintegrasi akan menambah kompleksitas data pasien dan penyedia layanan kesehatan sehingga perlu tata pamong untuk mengelola data tersebut. Hal yang perlu dipertimbangkan dalam tata pamong *Integrated Electronic Health Record* adalah pentingnya keamanan data pasien. Tata pamong Digital *Transformation Office* Kementerian Kesehatan Indonesia perlu untuk menyusun *framework* spesifikasi keamanan data untuk *microservice* data. Sehingga, Penulis menyusun rekomendasi spesifikasi

keamanan data untuk *microservice* data di *Digital Transformation Office (DTO)* Kementerian Kesehatan Indonesia.

2. TINJAUAN PUSTAKA

2.1 Integrated Electronic Health

Integrated Electronic Health mengacu pada integrasi tanpa batas dan *interoperabilitas* dari berbagai sistem dan teknologi kesehatan elektronik dalam organisasi pelayanan kesehatan atau di berbagai organisasi pelayanan kesehatan. Ini melibatkan kemampuan sistem kesehatan elektronik yang berbeda, seperti catatan kesehatan elektronik (EHR), sistem laboratorium, sistem pencitraan, dan sistem informasi kesehatan lainnya, dalam rangka bertukar data dan komunikasi secara efektif. Integrasi ini memungkinkan untuk berbagi dan mengakses informasi pasien, koordinasi perawatan, dan peningkatan efisiensi dan kualitas pemberian pelayanan kesehatan (Konnoth, 2022).Dalam sektor kesehatan, setiap penyedia layanan memiliki perangkat lunak dan format data yang berbeda-beda, sehingga data kesehatan nasional tersebar di berbagai penyedia. Untuk mengatasi situasi ini, Kementerian Kesehatan RI harus mengembangkan *platform* yang menghubungkan seluruh pemangku kepentingan di bidang Kesehatan dengan tujuan untuk menciptakan sumber data Kesehatan nasional yang terpercaya. Pendekatan ini tidak bertujuan untuk menggantikan aplikasi yang sudah ada, namun untuk mengintegrasikan berbagai aplikasi tersebut dengan aman melalui *otentikasi* dan enkripsi. *Platform* yang digunakan menggunakan prinsip *Open API* berbasis *Microservice* yang mana dapat mendukung kolaborasi antar pelaku industri kesehatan dengan menyediakan *platform* yang terbuka dan *interoperabilitas*. Dengan menggunakan *Open API*, berbagai aplikasi dan sistem kesehatan dapat saling terhubung dan berbagi data dengan mudah. Hal ini memungkinkan pengembangan teknologi pelayanan kesehatan yang lebih inovatif dan efisien, serta memperluas aksesibilitas bagi pasien. Dengan kolaborasi yang lebih baik, pelaku industri kesehatan dapat bekerja bersama untuk meningkatkan kualitas pelayanan kesehatan dan mencapai tujuan bersama.

2.2 Tata Pamong Satu Data

Tata pamong satu data biasanya mengacu pada manajemen terpusat dan kontrol data dalam suatu organisasi atau sistem. Ini melibatkan pendekatan terpadu dan konsisten untuk tata kelola data, manajemen data, dan praktik administrasi data. Dengan pendekatan administrasi data tunggal, terdapat otoritas pusat yang bertanggung jawab untuk menentukan standar data, memastikan kualitas data, menetapkan kebijakan dan prosedur data, serta mengelola akses dan keamanan data. Ini membantu memastikan konsistensi, akurasi, dan integritas data di berbagai aplikasi, *database*, dan sistem dalam organisasi. Ini juga memfasilitasi pembagian, integrasi, dan analisis data yang efisien, guna pengambilan keputusan yang tepat dan efektivitas operasional (Konnoth, 2022). *Platform as a Service* (*PaaS*) dapat menjadikan pendekatan yang efektif untuk menginvestasikan tata pamong satu data kesehatan nasional. Dengan *PaaS*, infrastruktur dan lingkungan pengembangan sudah tersedia, sehingga memungkinkan pengembang fokus pada pengembangan aplikasi kesehatan yang inovatif. *PaaS* juga dapat menyediakan *skalabilitas* dan keamanan yang diperlukan untuk mengelola data kesehatan nasional dengan efisien.

2.3 Data Security

Keamanan data mengacu pada perlindungan data dari akses, penggunaan, pengungkapan, perubahan, atau penghancuran yang tidak sah. Ini melibatkan penerapan langkah-langkah dan perlindungan untuk memastikan kerahasiaan, integritas, dan ketersediaan data. Keamanan data bertujuan untuk mencegah individu atau entitas yang tidak berwenang mendapatkan akses ke informasi sensitif atau rahasia, serta untuk mencegah pelanggaran data, kehilangan data, atau korupsi data. Langkah-langkah keamanan data biasanya meliputi:

1. Kontrol akses: Menerapkan mekanisme *otentikasi* dan otorisasi untuk memastikan yang berwenang yang akses data.
2. Enkripsi: Menggunakan teknik enkripsi untuk mengubah data menjadi bentuk kode yang hanya dapat diakses dengan kunci deskripsi yang sesuai.
3. *Firewall* dan keamanan jaringan: Menyebarkan *firewall* dan tindakan keamanan jaringan lainnya untuk melindungi data dari akses tidak sah melalui jaringan.
4. Pencadangan dan pemulihan data: Mencadangkan data secara teratur dan memiliki mekanisme untuk memulihkan data jika terjadi kehilangan data atau kegagalan sistem.
5. Kebijakan dan prosedur keamanan: Menetapkan kebijakan dan prosedur keamanan yang jelas yang menguraikan bagaimana data harus ditangani, disimpan, dan dilindungi.
6. Pelatihan dan kesadaran karyawan: Mendidik karyawan tentang praktik terbaik keamanan data dan meningkatkan kesadaran tentang potensi ancaman keamanan, seperti serangan *phishing* atau rekayasa sosial.
7. Audit dan penilaian keamanan reguler: Melakukan penilaian dan audit reguler untuk mengidentifikasi kerentanan dan memastikan kepatuhan terhadap standar dan peraturan keamanan data.

Dengan mengambil tindakan keamanan data yang kuat, organisasi dapat mengurangi risiko pelanggaran data, melindungi informasi sensitif, menjaga kepercayaan pelanggan, dan mematuhi peraturan perlindungan data.

3. METODE PENELITIAN

Dalam penelitian ini, digunakan pendekatan kualitatif dengan analisis dokumen. Metode penelitian ini didasarkan pada filsafat kondisi *postpositivisme* (Sugiyono, 2011). Metode ini digunakan untuk mempelajari kondisi objek alami. Peneliti berfungsi sebagai alat utama. Pengumpulan sampel data dilakukan secara *purposive* dan *snowball*, dan triangulasi digunakan. Dalam penelitian kualitatif, analisis data dilakukan secara induktif atau kualitatif, dengan fokus pada makna daripada generalisasi. Dalam penelitian ini, data yang jelas dikumpulkan untuk memperoleh informasi terkait objek penelitian. Data yang digunakan berasal dari sumber sekunder. Sedangkan analisis dokumen adalah prosedur sistematis untuk meninjau dan mengevaluasi dokumen dalam bentuk cetak atau elektronik (Fraenkel & Wallen, n.d.). Objek penelitian dalam hal ini adalah analisis dokumen *DTO (Digital Transformasi Office)* Kementrian Kesehatan Republik Indonesia. Objek penelitian merujuk pada atribut, sifat, atau nilai dari individu (Sugiyono, 2017). Data sekunder digunakan dalam penelitian ini, berupa *Health Digital Transformation Strategy Blueprint* 2024 dari *Website* Kementerian Kesehatan dan Laporan Tahunan 2022. Data sekunder ini digunakan sebagai latar belakang penelitian, gambaran umum terkait dengan *DTO* Kemenkes RI, serta menjadi dasar untuk menjawab permasalahan penelitian.

4. HASIL DAN PEMBAHASAN

4.1 Arsitektur Data Kementerian Kesehatan

Arsitektur data di Kementerian Kesehatan bertujuan untuk mengatur standarisasi data agar aplikasi dan data dapat terintegrasi dengan baik. Tujuannya adalah agar organisasi di tingkat kota, kabupaten, provinsi, nasional, dan global dapat menggunakan data dari berbagai aplikasi dan sistem informasi. Kementerian Kesehatan telah membuat kerangka standar untuk memastikan konsistensi dan *interoperabilitas* data. Dalam lingkungan pelayanan kesehatan, dua kerangka kerja yang digunakan adalah *Fast Healthcare Interoperability Resources* (FHIR) dan *open EHR*. Kementerian Kesehatan menggunakan REST API untuk pertukaran data FHIR seperti informasi klinis, rencana tata laksana, dan diagnosis. FHIR memiliki lebih dari 100 sumber daya yang dapat digunakan untuk membangun basis data sesuai kebutuhan. Selain itu, platform data terbuka EHR

menawarkan set elemen data yang lengkap dengan menggunakan lebih dari 300 arketipe yang berfokus pada konsistensi data.

Platform yang dikembangkan oleh *DTO* Kementerian Kesehatan, khususnya *one health systems*, tidak menggantikan sistem informasi yang sudah ada. Oleh karena itu, kerangka *interoperabilitas* data harus dapat disesuaikan dengan kebutuhan pengguna. *One health systems* memiliki dua *platform* utama, yaitu *Citizen Health App* dan *Partner Systems*. *Citizen Health App* digunakan untuk mengumpulkan data rekam medis elektronik pribadi pasien dan keluarganya. Data ini akan disimpan dalam basis data elektronik yang terpusat, dengan pulau-pulau data lain sebagai pendukungnya. Data rekam medis ini mencakup informasi tentang aktivitas pelayanan kesehatan seperti pemeriksaan, tindakan medis, dan prosedur klinis. Pulau data *Fasyankes* menyediakan informasi tentang penyedia layanan kesehatan seperti rumah sakit, puskesmas, klinik, dan laboratorium. Pulau data sumber daya manusia kesehatan yang terlibat dalam aktivitas layanan kesehatan. Pulau data pembiayaan berisi informasi tentang biaya yang timbul dari penanganan medis. Data rekam medis ini akan dilindungi oleh kerangka kerja perlindungan keamanan data yang disebut *data ownership and stewardship*. *Consent* akan menjadi bagian penting dalam pertukaran data, bersama dengan *metadata* dan data itu sendiri. Penggunaan *consent of the people* sebelum pengumpulan dan pengolahan data pribadi juga menjadi bagian penting dalam undang-undang perlindungan privasi dibanyak negara. Data yang sudah terintegrasi dan terstandarisasi akan didukung oleh analisis lanjutan seperti *text mining* dan *forecasting* menggunakan teknologi *big data analytics* terkini. Hal ini bertujuan untuk meningkatkan pelayanan kesehatan di Indonesia melalui *data mart* yang terupdate secara *real-time*.

4.2 Keamanan Data pada *Electronic Medical Record* Kementerian Kesehatan

Di sektor kesehatan terdapat berbagai aspek tantangan seperti pengumpulan data, keamanan, dan privasi, integrasi *electronic health record*, berbagi data, data tidak terstruktur, *autentikasi* data, dan ketersediaan data secara *realtime* (Rahul & Banyal, 2020). Aspek keamanan sistem dan perlindungan data pribadi menjadi prioritas Kemenkes RI dalam integrasi sistem. Pada *blueprint* strategi transformasi digital kesehatan 2024 *electronic medical record* dilindungi oleh perlindungan keamanan data *ownership* dan *stewardship* (Kementerian Kesehatan Republik Indonesia, 2023). Akan tetapi skema perlindungan keamanan data ini tidak terlihat pada laporan tahunan *digital transformation office* 2021-2022 Kementerian Kesehatan. Beberapa metode yang digunakan untuk melindungi informasi personal dan privasi pasien berdasarkan data kesehatan yaitu melalui *privacy protection laws, De-identification, differential privacy, perturbation, data centric approach, walled garden method, jujutsu security,* dan *HyberEx* (Gupta et al., 2023).

DTO Kementerian Kesehatan dapat menggunakan *general data protection regulation* yang diterbitkan oleh *European Union* di tahun 2018 yang mana menyediakan *framework* dasar untuk memproteksi informasi privat pribadi (Kementerian Kesehatan Republik Indonesia, 2023). Kanada menggunakan *The Personal Information Protection and Electronic Data Act* (PIPEDA). Undang-undang ini memberlakukan berbagai peraturan terkait pengumpulan, penyimpanan dan penggunaan data pribadi. Pemerintah Korea Selatan memberlakukan *Personal Information Protection Act* tahun 2011 dengan fokus utama melindungi data pribadi dari berbagai perusahaan yang tidak diotorisasi, penggunaan ilegal dan kebocoran data pribadi. Argentina menerapkan the 2000 *personal data protection act* yang digunakan untuk melindungi data pribadi masyarakat. Semua data kecuali nama, usia dan alamat termasuk dalam kategori data pribadi, bahkan *cookie* dianggap sebagai data pribadi. Pemerintah Australia menggunakan *Privacy Principles* yang menggabungkan 13 prinsip berbeda untuk mengelola data pribadi.

De-identifikasi adalah proses memberikan keamanan dari ketidakjelasan yaitu semua informasi yang secara khusus mengidentifikasi pasien dihapus dari data perawatan kesehatan berbasis *B2B*. Pemerintah Amerika Serikat menentukan serangkaian identifikasi

yang harus dihapus dari perawatan kesehatan berbasis *B2B* untuk memberikan diidentifikasi. *Differential privacy* memberikan kendali oleh pemilik data terhadap *kueri* masukan. *Differential privacy* menggunakan transformasi Laplace, dan metode eksponensial untuk membatasi respons *kueri* masukan. Metode keempat adalah *perturbation*. Metode ini menambahkan *randomisasi* ke data. Menambahkan *noise* atau menukar item data adalah metode yang umum digunakan untuk menciptakan gangguan. Selanjutnya adalah *data centric approac*h. Pendekatan ini diimplementasikan pada *gateway* dan pusat jaringan. *Walled garden method* salah satu metode keamanan yang diterapkan pada lapisan aplikasi. *Input* jaringan dikendalikan oleh kontrol akses dan *firewall*. Teknik jujutsu mengamankan data kesehatan dengan menggunakan mesin rekomendasi untuk merekomendasikan data yang direkomendasikan beserta kerentanannya. Metode terakhir adalah dengan menggunakan *HybrEx model* yang menggunakan *public cloud* dan *private cloud* secara simultan. Semua informasi sensitif disimpan di *private cloud*, sementara informasi lainnya disimpan d*i public cloud*.

DTO Kementerian Kesehatan (Kemenkes) memiliki fokus utama pada penyediaan layanan kesehatan terintegrasi melalui aspek keamanan Satusehat *mobile*. Untuk melindungi data, Kemenkes menggunakan metode *masking* dan enkripsi sehingga hanya pihak berkepentingan yang dapat mengaksesnya. Keamanan aplikasi Satusehat *mobile* akan terus diperbaharui sesuai dengan standar keamanan yang ditetapkan oleh BSSN. *DTO* Kemenkes menilai tujuh aspek keamanan informasi dalam *platform* Satusehat, termasuk tata Kelola, teknologi dan operasi, perlindungan data, pengelolaan pihak ketiga, sumber daya manusia, manajemen krisis, dan kepatuhan. Data kesehatan yang besar rentan akan adanya pelanggaran data atau kebocoran data mengakibatkan informasi pribadi sensitif pasien tersebar. Langkah-langkah keamanan yang tepat perlu diterapkan pada sistem mereka dengan beberapa teknologi diantaranya adalah *autentikasi*, akses kontrol, dan enkripsi. Protokol *autentikasi* tiga faktor untuk para profesional medis dapat mengakses data yang disimpan di *cloud server* (Dhillon & Kalra, 2018). Untuk meningkatkan keamanan, digunakan prinsip *autentikasi* berbasis kata sandi, berbasis biometrik, dan berbasis kartu pintar. Protokol *autentikasi* tiga faktor berbasis biometrik untuk komunikasi yang aman antara *Telecare Medical Information System (TMIS)* dan pasien (Kumari & Renuka, 2021). Protokol ini menggunakan kriptografi kurva eliptik. Metode lain yang digunakan untuk mencegah adanya pelanggaran data atau kebocoran data adalah akses kontrol. Metode ini memberikan *autentikasi* kepada penyedia layanan kesehatan berdasarkan data besar *B2B*. Setiap pengguna memiliki beberapa hak akses yang ditentukan oleh kebijakan kontrol akses. Terdapat beberaka akses kontrol yang dapat digunakan yaitu *rolebased access control*, *attributebased access control*, *policybased access control*, dan *auditbased access control* (Gupta et al., 2023). Metode enkripsi kunci publik yang dapat dicari untuk pengumpulan data jarak jauh, pelacakan gerakan, komunikasi antar tenaga medis(Ma et al., 2018). Skema enkripsi yang dapat dicari untuk skema berbagai data kesehatan elektronik. Dalam skema tersebut, data kesehatan elektronik disimpan di *server cloud* tetapi indeksnya disimpan di *blockchain* (Chen et al., 2019).

5. KESIMPULAN

Peraturan Menteri Kesehatan Republik Indonesia No. 21 Tahun 2020 mengenai Rencana Strategis Kementerian Kesehatan Tahun 2020-2024 mewajibkan perubahan dalam tata kelola pembangunan kesehatan, termasuk integrasi sistem(Kementerian Kesehatan Republik Indonesia, 2021). Untuk mencapai integrasi sistem dan pengembangan satu data rekam medis, diperlukan tata pamong yang baik dalam mengatur kebijakan terkait data tersebut. Implementasi sistem satu data kesehatan berbasis individu, seperti rekam medis elektronik terintegrasi, di Kementerian Kesehatan akan menghasilkan *big* data yang dapat dianalisis untuk keperluan prediksi dan analisis kesehatan

Masyarakat Indonesia. Tantangan utama analisis data dalam industri kesehatan adalah struktur data, keamanan, standardisasi data, penyimpanan dan transfer, manajerial keterampilan seperti tata pamong data. *Platform* yang dikembangkan *DTO* Kementerian Kesehatan adalah Satudata Kesehatan (Kruse et al., 2016). Data rekam medis akan mendapatkan perlindungan melalui suatu kerangka kerja yang disebut data *ownership and stewardship*, yang bertujuan untuk menjaga keamanan data tersebut. *Consent* akan menjadi salah satu bagian penting dalam setiap proses pertukaran data, bersama dengan *metadata* dan data itu sendiri. Kementerian Kesehatan Republik Indonesia memberikan prioritas pada aspek keamanan sistem dan perlindungan data pribadi dalam integrasi sistem yang dilakukan. Namun, laporan tahunan digital transformasi Kementerian Kesehatan tahun 2021-2022 tidak mencantumkan skema perlindungan keamanan data ini secara rinci.

DTO Kemenkes memprioritaskan keamanan Satusehat *mobile* sebagai layanan kesehatan terintegrasi dengan menggunakan metode *masking* dan enkripsi data. Aplikasi Satusehat *mobile* akan terus diperbaharui sesuai dengan standar keamanan yang ditetapkan oleh BSSN. *DTO* Kemenkes mengevaluasi tujuh aspek keamanan informasi dalam *platform* Satusehat, termasuk tata kelola, teknologi dan operasi, perlindungan data, pengelolaan pihak ketiga, sumber daya manusia, manajemen krisis dan kepatuhan. Data kesehatan yang besar rentan akan adanya pelanggaran data atau kebocoran data mengakibatkan informasi pribadi sensitif pasien tersebar. Langkah-langkah keamanan yang tepat perlu diterapkan pada sistem mereka dengan beberapa teknologi diantaranya adalah *autentikasi*, akses kontrol, dan enkripsi.

DAFTAR PUSTAKA

Chen, L., Lee, W. K., Chang, C. C., Choo, K. K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems*, *95*, 420–429. https://doi.org/10.1016/j.future.2019.01.018

Dhillon, P. K., & Kalra, S. (2018). Multi-factor user authentication scheme for IoT-based healthcare services. *Journal of Reliable Intelligent Environments*, *4*(3), 141–160. https://doi.org/10.1007/s40860-018-0062-5

Fanelli, S., Pratici, L., Salvatore, F. P., Donelli, C. C., & Zangrandi, A. (2023). Big data analysis for decision-making processes: challenges and opportunities for the management of health-care organizations. *Management Research Review*, *46*(3), 369–389. https://doi.org/10.1108/MRR-09-2021-0648

Fraenkel, J. R., & Wallen. (n.d.). How to design and evaluate research in education (6th ed. *McGraw-Hill*.

Gupta, B. B., Gaurav, A., & Kumar Panigrahi, P. (2023). Analysis of security and privacy issues of information management of big data in B2B based healthcare systems. *Journal of Business Research*, *162*. https://doi.org/10.1016/j.jbusres.2023.113859

Holly, L., Thom, S., Elzemety, M., Murage, B., Mathieson, K., & Iñigo Petralanda, M. I. (2023). Strengthening health data governance: new equity and rights-based principles. *International Journal of Health Governance*. https://doi.org/10.1108/IJHG-11-2022-0104

Kementerian Kesehatan Republik Indonesia. (2021). *Cetak Biru Strategi Transformasi Digital Kesehatan 2024*.

Kementerian Kesehatan Republik Indonesia. (2023). *Membangun Integrasi Menuju Transformasi Digital Kesehatan: Laporan Tahunan Digital Transformation Office 2021-2022*.

Konnoth, C. (2022). Are Electronic Health Records Medical Devices? In *The Future of Medical Device Regulation* (pp. 36–46). Cambridge University Press. https://doi.org/10.1017/9781108975452.004

Kruse, C. S., Goswamy, R., Raval, Y., & Marawi, S. (2016). Challenges and opportunities of big data in health care: A systematic review. In *JMIR Medical Informatics* (Vol. 4, Issue 4). JMIR Publications Inc. https://doi.org/10.2196/medinform.5359

Kumari, S., & Renuka, K. (2021). Design of a Password Authentication and Key Agreement Scheme to Access e-Healthcare Services. *Wireless Personal Communications*, *117*(1), 27–45. https://doi.org/10.1007/s11277-019-06755-7

Ma, M., He, D., Khan, M. K., & Chen, J. (2018). Certificateless searchable public key encryption scheme for mobile healthcare system. *Computers and Electrical Engineering*, *65*, 413–424. https://doi.org/10.1016/j.compeleceng.2017.05.014

Rahul, K., & Banyal, R. K. (2020). Data Life Cycle Management in Big Data Analytics. *Procedia Computer Science*, *173*, 364–371. https://doi.org/10.1016/j.procs.2020.06.042

Sugiyono. (2011). *Metode Penelitian Kuantitaif Kualitatif dan R & D*. Alfabeta.
Sugiyono. (2017). *Metode penelitian kuantitatif, kualitatif dan R&D*. Alfabeta.