JUCOSCO | Vol.5 | No.1 | Januari 2025 | Hal. 13-22
Online ISSN : 2774-9037

This Journal is available in Universitas Bhayangkara Jakarta Raya online Journals

Journal of Computer Science Contributions (JUCOSCO)

Journal homepage: https://ejurnal.ubharajaya.ac.id/index.php/jucosco

Transformasi Digital Sektor Kesehatan Pada Telemedisin Indonesia

M. Yusuf Samad[1,*], Fajri Rosadi[2], Fatimah Azzahra[2], Taryana Brata[3], Diah Ayu Permatasari[4], Nova Teguh Krisdwiyanto[5]

[1] Communication & Information System Security Research Center (CISSReC), ahmadyusad@gmail.com
[2] Universitas Indonesia, rosadi@ui.ac.id, fatimah.zahra9@gmail.com
[3] Sekolah Tinggi Intelijen Negara, newerry3199@gmail.com
[4] Universitas Bhayangkara Jakarta Raya, pepy@ubharajaya.ac.id
[5] Universitas Nusa Putra, nova.teguh@nusaputra.ac.id

Abstract

Digital transformation in the health sector in Indonesia has grown since the COVID-19 pandemic several years ago, one form of digital transformation is the emergence of telemedicine services in Indonesia. However, Indonesia's capacity and readiness are not yet adequate for realizing digital transformation because Indonesia needs to anticipate several risks that may occur in accelerating digital transformation, such as the potential for data misuse and privacy violations and the threat of cyberattacks. This article aims to identify the challenges and opportunities for digital transformation, especially telemedicine services in Indonesia. This article uses a qualitative approach with data sources from literature reviews. The results show that digital transformation in the health sector, especially telemedicine services, faces challenges from people, processes, and technology. However, training medical personnel, increasing system integration, and using protection technology are opportunities to improve patient data security and the efficiency of telemedicine services.

Keywords— Telemedicine, Digital Transformation, Health.

Abstrak

Transformasi digital pada sektor kesehatan di Indonesia semakin berkembang sejak adanya pandemi COVID-19 yang terjadi beberapa tahun lalu, salah satu bentuk transformasi digital adalah munculnya layanan telemedisin di Indonesia. Namun, kapasitas dan kesiapan Indonesia belum mumpuni dalam mewujudkan transformasi digital karena Indonesia perlu mengantisipasi beberapa risiko yang mungkin terjadi dalam percepatan transformasi digital seperti potensi penyalahgunaan data dan pelanggaran privasi hingga ancaman serangan siber. Tulisan ini bertujuan untuk mengidentifikasi tantangan dan peluang transformasi digital khususnya layanan telemedisin di Indonesia. Tulisan ini menggunakan pendekatan kualitatif dengan sumber data berupa kajian literatur. Hasil menunjukkan bahwa transformasi digital di sektor kesehatan, khususnya layanan telemedisin dihadapkan pada tantangan *people*, *process*, dan *technology*. Namun, pelatihan tenaga medis, peningkatan integrasi sistem, dan penggunaan teknologi proteksi menjadi peluang untuk meningkatkan keamanan data pasien dan efisiensi layanan telemedisin.

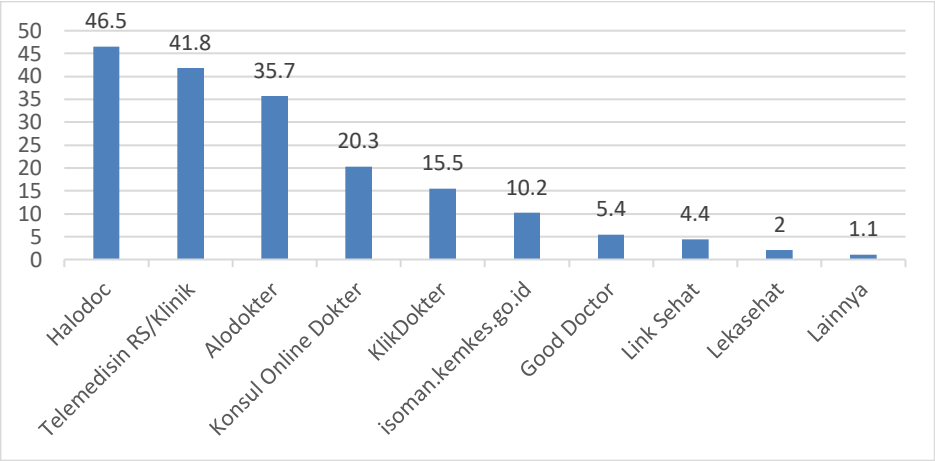
Kata kunci— Telemedisin, Transformasi Digital, Kesehatan.

Article info
Submitted (20/01/2025)
Revised (23/01/2025)
Accepted (29/01/2025)
Published (31/01/2025)
Korespondensi: ahmadyusad@gmail.com*

I. PENDAHULUAN

Situasi pandemi Covid-19 telah menjadi katalis terhadap akselerasi transformasi digital sehingga mengakibatkan adanya disrupsi di semua lini. Banyaknya kegiatan masyarakat yang bersentuhan dengan teknologi digital telah menjadikan masyarakat sebagai sasaran empuk kejahatan dunia digital. Ancaman serangan siber di masa kenormalan baru bukan hanya meningkatkan jumlah korban, tetapi juga meningkatkan kemampuan dalam menghampiri korbannya. (Wicaksana et al., 2020). Di sisi lain, perkembangan teknologi pada situasi pandemi juga mendorong penyebaran informasi positif untuk membantu satu sama lain untuk bertahan di masa pandemi (Samad & Azzahra, 2022).

Pemerintah Indonesia mencatat terjadi peningkatan akses terhadap layanan kesehatan jarak jauh atau aplikasi *telemedicine* (telemedisin) sebanyak 600 persen selama pandemi Covid-19 (Ansori, 2020). Selain itu, pada tahun 2022, hasil peninjauan dari Katadata Insight Center menunjukkan bahwa total pengguna baru layanan telemedisin mencapai 44,1% dalam rentan waktu satu semester terakhir. Selain itu, hasil lain yang ditunjukkan adalah sebanyak 1.416 diantaranya menggunakan layanan telemedisin seperti Halodoc, Alodokter, Good Doctor, Konsul Online Dokter, KlikDokter, isoman.kemkes.go.id, dan lainnya (Setyowati, 2022).



Sumber: Diolah penulis dari Setyowati (2022)

Gambar 1. Penggunaan layanan telemedisin dan fasilitas kesehatan di Indonesia dari yang paling popular hingga yang paling sedikit digunakan

Hasil studi Kaspersky tentang telemedisin dengan melakukan interviu kepada sebanyak 389 perwakilan penyedia layanan kesehatan di 34 negara termasuk ASEAN, Asia Pasifik, dan komunitas negara independen. Riset Kaspersky menunjukkan bahwa sebanyak 30 persen perusahaan penyedia layanan kesehatan pernah mengalami kasus keamanan data pasien kegiatan. Disamping itu, nyaris setengah dari penyedia layanan menyepakati fakta bahwa dokter tidak paham tentang perlindungan data pasien (Global Kaspersky Research, 2021).

Menteri Kesehatan Budi Gunadi Sadikin mengatakan bahwa terdapat berbagai kekurangan dari layanan

telemedisin berdasarkan laporan dari masyarakat, salah satunya adalah pasien diminta untuk membayar agar mendapat fasilitas kesehatan. (Evandio, 2022). Permasalahan tentang layanan dalam jaringan (daring) atau *online* Kementerian Kesehatan tidak hanya berkaitan dengan telemedisin saja, tetapi juga terkait dugaan kebocoran data 1,3 pengguna aplikasi e-HAC versi lawas, kebocoran data ini diduga berasal dari pihak mitra ketiga. Peneliti dari vpnMentor, mengungkapkan bahwa eHAC tidak memakai protokol privasi yang jelas sehingga menyebabkan jutaan data sensitif terungkao di peladen terbuka. Kondisi ini terjadi pada semua infrastruktur eHAC, termasuk data pribadi dari layanan kesehatan dan pejabat Indonesia yang memiliki aplikasi e-HAC (Nasution, 2021). Di sisi lain, Kementerian Kesehatan membantah telah terjadi kebocoran data dan telah menindaklanjuti kerentanan yang ditemukan oleh vpnMentor di platform mitra (Widyawati, 2021).

Dugaan kebocoran lainnya adalah data yang dimiliki oleh Kemenkes dengan detail data yang dijual berupa data enam juta sampel dengan kapasitas sebesar 720 GB. Pelaku merinci sampel data diantaranya keluhan pasien, surat rujukan Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, rumah sakit, laporan radiologi, foto pasien, surat persetujuan menjalani isolasi untuk Covid, nama lengkap pasien, keluhan pasien, hasil tes laboratorium, hasil pindai X-Ray. Kemenkes dan Kementerian Komunikasi dan Informatika berkoordinasi dan melakukan penelusuran dugaan kasus kebocoran tersebut (Rizkinaswara, 2022).

Dalam Pasal 57 Undang-Undang Kesehatan menegaskan bahwa pasien berhak atas privasi terkait kondisi kesehatan pribadi yang telah diserahkan kepada penyedia layanan kesehatan, kecuali ada ketentuan lain yang dijelaskan secara jelas dalam pasal tersebut, yang mencakup kondisi dan pihak-pihak yang terlibat (Mahira, 2021). Sementara itu, Pasal 47 Ayat (2) Undang-Undang Praktik Kedokteran mengharuskan dokter dan pengelola fasilitas kesehatan untuk menjaga kerahasiaan informasi medis setiap individu, termasuk dokumen dan catatan terkait informasi kesehatan yang diberikan kepada pasien. Dalam kaitannya dengan perlindungan data pribadi di sektor kesehatan, Pasal 26 UU ITE mengatur bahwa pemanfaatan data pribadi dan informasi elektronik yang berkaitan dengan data pribadi seseorang di Indonesia harus dilakukan dengan persetujuan individu tersebut atau berdasarkan dasar hukum yang sah sebagai bentuk pengolahan data yang sah (Utomo, Gultom, & Afriana, 2020). Hal serupa juga diatur dalam Undang-Undang Perlindungan Data Pribadi yang secara khusus mencakup data kesehatan.

Berdasarkan sejumlah aturan hukum diatas, sudah sepatutnya penyedia layanan telemedisin sebagai bagian dari badan publik wajib melindungi data pribadi pasien atau pengguna layanan kesehatan. Namun, pada praktiknya, data pasien tidak sepenuhnya terlindungi karena beberapa kali terjadi dugaan insiden kebocoran data di Kementerian Kesehatan. Kebocoran data pada layanan telemedisin berpotensi terjadi mengingat adanya dugaan kasus serangan siber berupa dugaan

kebocoran data sehingga penulis menilai perlu dilakukan kajian tentang ancaman siber yang berpotensi terjadi pada layanan telemedisin Kementerian Kesehatan.

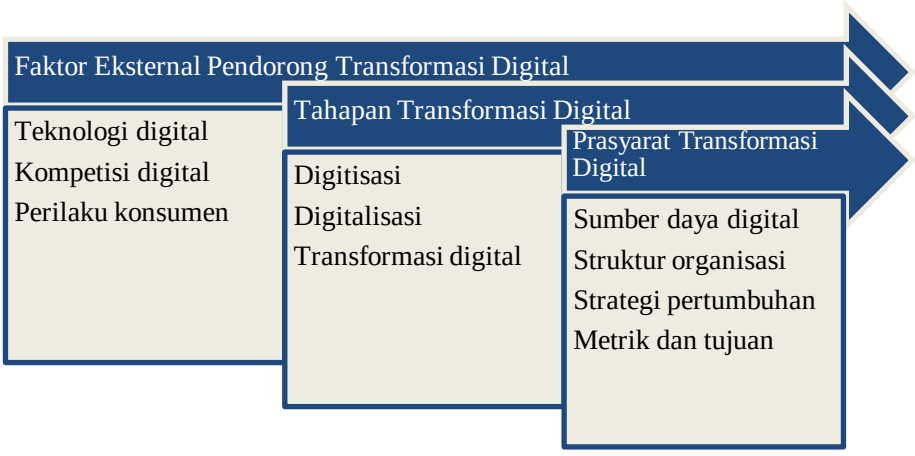
II. METODE PELAKSANAAN

Desain studi yang digunakan berupa desain kualitatif dengan data yang bersumber dari literatur-literatur seperti artikel ilmiah yang dimuat dalam jurnal, berita, hingga dokumen nasional. Desain ini menyediakan berbagai mekanisme yang berguna dalam pengecekan bagaimana manusia mengetahui dunianya (Potter, 2013). Studi ini juga dilakukan terhadap pengaturan dan pengawasan terhadap kerahasiaan data pribadi dan penggunaan teknologi informasi di bidang kesehatan di Indonesia. Indonesia. Pengamatan yang dilakukan terhadap tren data kesehatan dan pelanggaran data kesehatan dalam penggunaan layanan medis online yang banyak digunakan di Indonesia saat ini. Kemudian hasil pengamatan dan studi literatur tersebut disandingkan dengan teori dan konsep yang digunakan pada studi ini.

III. HASIL DAN PEMBAHASAN

III.1. Transformasi Digital

Riset yang dilakukan oleh Verhoef et al., (2021) menggagas serangkaian tahapan untuk menginterpretasikan transformasi digital yang dibagi menjadi tiga perspektif pokok, yaitu faktor pendorong, tahapan transformasi, dan prasyarat utama, seperti yang dijelaskan pada gambar di bawah ini.



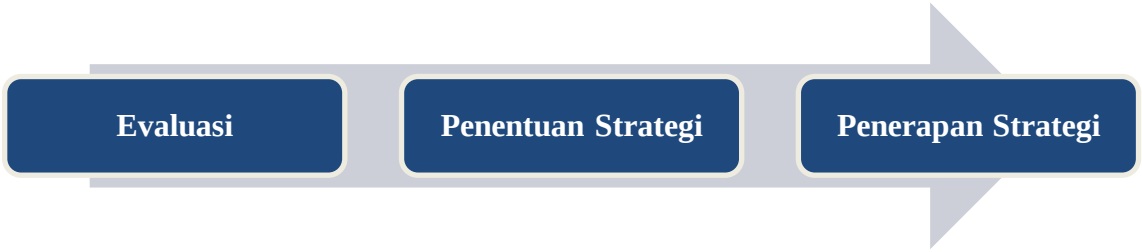
Sumber: Diolah penulis dari Verhoef et al., (2021)

Gambar 2. Tahapan memahami transformasi digital dimulai dari faktor eksternal pendorong transformasi digital hingga prasyarat transformasi digital.

Gambar 1 menunjukkan bahwa bahwa salah satu faktor utama yang mendorong adanya transformasi digital adalah perkembangan teknologi digital itu sendiri. Ini mencakup semakin luasnya penggunaan

world wide web (www), akses internet (termasuk teknologi *broadband*), telepon pintar, serta kemajuan teknologi yang lebih canggih seperti kecerdasan artifisial, pencetakan tiga dimensi, otomasi, robotika, *Internet of Things* (IoT), dan lainnya. Perkembangan teknologi digital ini telah memicu perubahan signifikan dalam proses bisnis di berbagai sektor yang pada akhirnya memengaruhi dinamika kompetisi serta perilaku konsumen yang juga mengalami perubahan besar (Verhoef et al., 2021).

Sebuah tinjauan literatur yang dilakukan oleh Zaoui & Souissi (2020) menyoroti perlunya upaya bersama dan refleksi serius pada proses transformasi digital. Menurut studi tersebut, terdapat tiga pilar mendasar yang membentuk proses transformasi digital, yaitu: mengevaluasi, menentukan strategi, dan menerapkannya.



Sumber: Zaoui & Souissi (2020)

Gambar 2. Alur proses transformasi digital dimulai dari tahapan evalausi kemudian dilanjutkan dengan penetuan strategi dan yang terakhir adalah penerapan strategi

Alur proses transormasi digital diatas telah digunakan untuk mengkaji kebijakan penggunaan aplikasi PeduliLindungi atau SATUSEHAT Mobile milik Kementerin Kesehatan. Hasil studi tersebut menunjukkan bahwa terdapat potensi ancaman keamanan nasional pada aplikasi yang diteliti. Potensi itu ada pada kelemahan penerapan *Cyber Threat Intelligence* (CTI) dan penerapan pilar keamanan siber yang dapat dimanfaatkan sebagai celah dalam melakukan serangan siber. Selain itu, potensi ancamannya dapat berkembang pada aspek sosial-politik, pertahanan-keamanan, dan aspek keamanan lainnya. Dari data yang ada pada aplikasi tersebut, dapat mengancam berbagai aspek keamanan nasional jika tidak dikelola dengan baik karena apabila data-data kesehatan tersebut bocor, maka potensi ancamannya berdampak pada segala aspek. Upaya antisipasi ancaman keamanan nasional seperti deteksi dini dan peringatan dini dalam keamanan siber, pemetaan ancaman, dan pembentukan unit khusus perlindungan data menjadi penting untuk .diterapkan untuk memaksimalkan proses transformasi digital kesehatan Indonesia (Samad, Persadha, & Suhardi, 2024).

III.2. Keamanan Siber Sektor Kesehatan

Berdasarkan riset yang berjudul "*Digital Healthcare - Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations*", terdapat lima jenis serangan siber teratas di Asia khususnya pada layanan kesehatan, mulai dari *phising* dengan cara mengirimkan tautan berbahaya melalui email, *ransomware* dengan cara mengenkripsi data dan

permintaan tebusan, *Advanced Persistent Threat (APT)* dengan cara instalasi eksfiltrasi data atau data terenkripsi, *trojan* dengan cara instalasi *backdoor* dan mengakses sistem, dan *malware* dengan cara memata-matai sistem atau akses data (Kandasamy, Srinivas, Achuthan, & Rangan, 2022).

Sebuah riset menemukan bahwa masyarakat memiliki tingkat kepercayaan yang tinggi terhadap telemedisin. Riset itu menemukan bahwa pembentukan kepercayaan terhadap layanan telemedisin ditentukan oleh beberapa faktor kepercayaan multidimensi yang dapat saling mempengaruhi satu sama lain. Faktor utamanya adalah kepercayaan pada organisasi perawatan, kepercayaan pada perawatan profesional, kepercayaan pada perawatan, dan kepercayaan pada teknologi. Faktor lain yang menentukan kepercayaan terhadap telemedisin adalah karakteristik individu, seperti usia, jenis kelamin, tingkat pendidikan melek teknologi, pendapatan, jenis penyakit, kondisi kesehatan, frekuensi penggunaan, dan pengalaman. Selain itu, terdapat faktor-faktor di luar karakteristik individu yang juga dapat menentukan kepercayaan terhadap telemedisin, seperti dukungan keluarga, tempat tinggal, komunitas, dan media sosial, pandemi Covid-19, serta adanya kebijakan dan regulasi yang mendukung dan ditegakkan (Purnastyasih & Prasojo, 2023).

Cyber medicine adalah penyebaran informasi pasien klinis dan nonklinis yang dapat disalahgunakan untuk kepentingan pribadi yang berujung merugikan orang lain. Hal ini dapat terjadi karena aktivitas telemedisin berbasis online, sehingga ada kemungkinan terjadi kebocoran data. Layanan kesehatan diharapkan dapat mengoptimalkan sistem keamanan dan meningkatkan sumber daya manusia yang kompeten untuk menerbitkan rekam medis elektronik yang terintegrasi dengan baik untuk menciptakan rasa aman bagi pasien. Bagi para dokter dan tenaga kesehatan, saran yang dapat diberikan adalah agar dapat mencontoh berbagai ancaman yang muncul dari berbagai kemampuan dan menjalankan kewenangan dengan penuh tanggung jawab. Mengingat pasien adalah pihak yang harus menjaga kerahasiaan dan keamanan informasinya. (Yuninda, Pasma, & Mantoro, 2022).

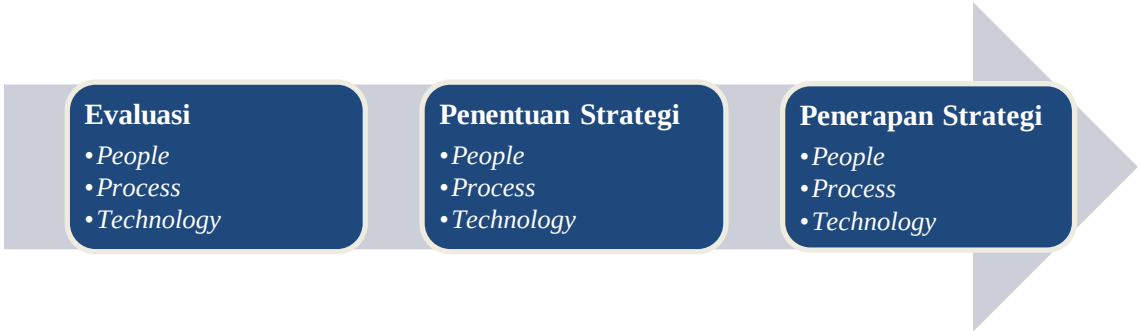
Masalah yang tidak kalah penting terkait dengan teknologi telemedisin adalah keamanan. Keamanan merupakan hal yang harus dipenuhi karena teknologi Telemedicine berjalan dalam jaringan internet. Dengan adanya keamanan teknologi telemedisin juga akan mempengaruhi tingkat kepercayaan masyarakat terhadap penerapan telemedisin (Kurniawan, 2016). Implementasi telemedisin di Indonesia telah memunculkan sejumlah catatan penting, termasuk kemampuan teknologi, keamanan data, privasi pasien, kerangka hukum dan peraturan, resistensi dari dokter dan pasien, dan biaya yang terkait dengan layanan telemedicine. Khususnya, keamanan data pasien dalam telemedicine menjadi perhatian utama; keamanan sistem yang tidak memadai membuat platform ini rentan terhadap peretasan, yang berpotensi memungkinkan penjahat siber untuk mencuri informasi pasien yang sensitif selama konsultasi. Data medis yang dicuri tersebut sering kali dijual di pasar gelap untuk tujuan jahat (Fakih, 2022) Dari aspek hukum,

III.3. Tantangan dan Peluang Transformasi Digital Layanan Telemedisin

Tulisan ini mengadopsi tantangan transformasi digital yang digagas oleh Teoh, dkk (2018). Teoh, dkk. (2018) menjabarkan tantangan dalam mengimplementasikan keamanan siber dalam sebuah organisasi. Tantangan tersebut dibagi menjadi tiga pilar, yakni sumber daya manusia (*people*), proses (*process*), dan teknologi (*technology*). Pada aspek *people*, kepercayaan masyarakat terhadap layanan telemedisin dipengaruhi oleh berbagai faktor, termasuk kepercayaan pada perawatan profesional dan organisasi. Kepercayaan ini sangat tergantung pada kompetensi tenaga kesehatan dalam menangani data pribadi pasien dan memastikan bahwa sistem teknologi informasi yang digunakan aman. Jika tenaga medis atau staf kesehatan tidak dilatih dengan baik mengenai ancaman siber, seperti *phishing*, *ransomware*, dan *malware*, maka celah keamanan akan terbuka.

Pada aspek *process*, seiring berkembangnya teknologi, banyak sistem yang tidak terintegrasi dengan baik dalam organisasi kesehatan, yang dapat mempengaruhi pengelolaan data dan kerentanannya terhadap ancaman. Data rekam medis elektronik yang tersebar tanpa kontrol yang baik akan lebih rentan disusupi oleh *trojan* atau *malware*. Kasus dugaan kebocoran data kesehatan menunjukkan bahwa pengelolaan data yang tidak kompeten. Selanjutnya, pada aspek *technology*, Telemedisin dan *cyber medicine* sering kali mengandalkan teknologi berbasis *cloud* dan sistem komunikasi online untuk menyimpan dan mengirimkan data pasien. Risiko kebocoran data atau pengaksesan data secara ilegal meningkat seiring dengan penggunaan sistem yang tidak aman. Penggunaan teknologi seperti enkripsi yang kuat, *firewall*, dan autentikasi ganda sangat penting untuk melindungi data ini.

Jika merujuk pada proses transformasi digital Zaoui & Souissi (2020), maka setiap aspek dilakukan evaluasi, penentuan strategi dan implementasi strategi. Dengan pilar-pilar ini, proses transformasi digital tidak hanya melibatkan teknologi, tetapi juga pemikiran strategis dan kemampuan organisasi untuk beradaptasi.



Gambar 2. Transformasi digital layanan telemedisin yang masing-masing alur proses disandingkan dengan aspek *people*, *process*, dan *technology*

Pada aspek *people*, kepercayaan masyarakat terhadap telemedisin sangat dipengaruhi oleh kompetensi tenaga kesehatan dan kemampuan mereka untuk menjaga keamanan data pribadi pasien. Keberhasilan

dalam aspek ini bergantung pada apakah tenaga medis terlatih dalam mengenali dan mengatasi ancaman siber seperti *phishing*, *ransomware*, dan *malware*. penting untuk mengevaluasi tingkat pengetahuan dan keterampilan tenaga medis terkait keamanan siber, merumuskan strategi pelatihan yang efektif, dan menerapkannya secara konsisten untuk memastikan mereka mampu melindungi data pasien dengan baik. Selanjutnya, pada aspek *process*, evaluasi terhadap sistem yang ada sangat penting agar dapat memastikan bahwa ada kontrol yang cukup terhadap alur data dan integrasi antar sistem. Strategi untuk mengintegrasikan sistem dan memitigasi potensi kebocoran data perlu diterapkan, seperti kebijakan enkripsi dan autentikasi yang lebih ketat. Implementasi sistem pengelolaan data yang lebih terintegrasi dan aman harus dilakukan dengan fokus pada pengamanan data rekam medis elektronik yang ada pada sistem penyimpanan layanan telemedisin. Terakhir, evaluasi terhadap keamanan sistem teknologi yang digunakan sangat penting dilakukan, evaluasi dapat dilakukan dalam bentuk penilaian keamanan dengan memanfaatkan layanan publik Badan Siber dan Sandi Negara dan Badan Intelijen Negara (Samad, 2021). Hasil evaluasi tersebut kemudian dijadikan dasar untuk menentukan strategi yang tepat mencakup penerapan teknologi perlindungan yang canggih. Implementasi teknologi ini harus dilakukan dengan cermat untuk memastikan bahwa data pasien terlindungi dengan aman dari ancaman siber.

IV. KESIMPULAN DAN SARAN

Transformasi digital sektor kesehatan khususnya layanan telemedisin menghadapi tantangan di tiga aspek utama, yaitu *people*, *process*, dan *technology*. Tantangannya meliputi rendahnya pemahaman tenaga medis tentang ancaman siber, integrasi sistem yang buruk, serta penggunaan teknologi yang rentan terhadap kebocoran data. Namun, hal ini juga membuka peluang untuk meningkatkan keamanan dengan pelatihan tenaga medis terkait ancaman siber, memperbaiki integrasi sistem pengelolaan data, serta menerapkan teknologi perlindungan seperti enkripsi, *firewall*, dan autentikasi ganda. Dengan evaluasi yang tepat dan strategi yang matang, transformasi digital dapat memperkuat keamanan data pasien, meningkatkan kepercayaan masyarakat, dan menciptakan sistem telemedisin yang lebih efisien dan aman. Program ini memiliki keterbatasan dari sisi sumber data yang masih minim sehingga tidak menggambarkan secara komprehensif mengenai tantangan dan peluang transformasi digital sektor kesehatan. Untuk itu, peneliti selanjutnya dapat melakukan riset dengan melakukan perbandingan setiap layanan telemedisin yang ada di Indonesia dengan menggunakan data-data primer.

Ucapan Terima Kasih

Penulis menyampaikan rasa terima kasih yang kepada semua peneliti, akademisi, dan penulis yang karyanya telah dirujuk dalam tinjauan pustaka ini. Penulis juga mengucapkan terima kasih kepada Universitas Bhayangkara Jakarta Raya atas kesediaannya dalam memproses artikel ini hingga pada tahap publikasi.

Referensi

Ansori, A. N. Al. (2020). Kominfo Perbaharui Aplikasi PeduliLindungi Guna Penguatan Layanan Telemedis di Masa COVID-19. *Liputan6*. Retrieved from https://www.liputan6.com/health/read/4441238/kominfo-perbaharui-aplikasi-pedulilindungi-guna-penguatan-layanan-telemedis-di-masa-covid-19

Evandio, A. (2022). Akui Layanan Telemedicine ada Kekurangan, Menkes: Adukan saja Keluhannya. *Kabar24*. Retrieved from https://kabar24.bisnis.com/read/20220214/15/1500272/akui-layanan-telemedicine-ada-kekurangan-menkes-adukan-saja-keluhannya

Fakih, M. (2022). Telemedicine in Indonesia During the Covid-19 Pandemic: Patient ' s Privacy Rights Protection Overview. *FIAT JUSTISIA: Jurnal Ilmu Hukum*, *16*(1), 1–17. https://doi.org/10.25041/fiatjustisia.v16no1.2583

Global Kaspersky Research. (2021). *Almost a third of clinicians have had their patients' data compromised when conducting remote telehealth sessions*. Retrieved from https://www.kaspersky.com/about/press-releases/2021_almost-a-third-of-clinicians-have-had-their-patients-data-compromised-when-conducting-remote-telehealth-sessions

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2022). Digital Healthcare - Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations. *IEEE Access*, *10*, 12345–12364. https://doi.org/10.1109/ACCESS.2022.3145372

Kurniawan, M. T. (2016). Culture and Security as Success Factors of Implement Telemedicine Technology: Case Study in Indonesia. *The 1'st International Conference on Green Development*. University of Jambi.

Mahira, A. N. (2021). Perlindungan Hukum Terhadap Kerahasiaan Data Kesehatan Pasien Berdasarkan Undang-Undang Nomor 36 Tahun 2009 Tentang Kesehatan. *Dinamika, Jurnal Ilmiah Ilmu Hukum*, *27*(10).

Nasution, A. D. (2021). Kemenkes Akui Dugaan Data eHAC Lama Bocor, Tak Terkait Peduli Lindungi. *Katadata*. Retrieved from https://katadata.co.id/ameidyonasution/berita/612dbf7f7528f/kemenkes-akui-dugaan-data-ehac-lama-bocor-tak-terkait-peduli-lindungi

Potter, W. J. (2013). *An Analysis of Thinking and Research About Qualitative Methods* (1st ed.). Routledge. https://doi.org/https://doi.org/10.4324/9780203811863

Purnastyasih, D., & Prasojo, E. (2023). The Determinant of Trust in Telemedicine: A Systematic Review. *Jurnal Kebijakan Dan Administrasi Publik*, *27*(1), 51–64. Retrieved from https://journal.ugm.ac.id/jkap/article/view/82724

Rizkinaswara, L. (2022). Kominfo Merespons Dugaan Kebocoran Data Milik Kemenkes. *Kementerian Kesehatan*. Retrieved from https://aptika.kominfo.go.id/2022/01/kominfo-merespons-dugaan-kebocoran-data-milik-kemenkes/

Samad, M. Y. (2021). Optimalisasi Layanan Publik Badan Intelijen Negara Dalam Perspektif Global Cybersecurity Index. *Al Ulum Sains Dan Teknologi*, *7*(1).

Samad, M. Y., & Azzahra, F. (2022). Penerapan Propaganda di Media Sosial Twitter Guna Menyebarkan Informasi Terkait Covid-19. *Jurnal Riset Manajemen Komunikasi*, *2*(2), 119–128.

https://doi.org/10.29313/jrmk.v2i2.1634

Samad, M. Y., Persadha, P. D., & Suhardi. (2024). Transformasi Digital Sektor Kesehatan Dalam Perspektif Keamanan Nasional. In *Transformasi Digital dan Daya Saing: Seleksi Kasus*. Yogyakarta: Gadjah Mada University Press.

Setyowati, D. (2022). Jumlah Pengguna Baru Layanan Telemedicine Capai 44% dalam 6 Bulan. *Katadata Insight Center*. Retrieved from https://katadata.co.id/digital/startup/624e9b8b96669/jumlah-pengguna-baru-layanan-telemedicine-capai-44-dalam-6-bulan

Teoh, C. S., Mahmood, A. K., & Dzazali, S. (2018). Cyber Security Challenges in Organisations: A Case Study in Malaysia. *2018 4th International Conference on Computer and Information Sciences: Revolutionising Digital Landscape for Sustainable Smart Society, ICCOINS 2018 - Proceedings*, 1–6. IEEE. https://doi.org/10.1109/ICCOINS.2018.8510569

Utomo, H. P., Gultom, E., & Afriana, A. (2020). Urgensi Perlindungan Hukum Data Pribadi Pasien Dalam Pelayanan Kesehatan Berbasis Teknologi Di Indonesia. *Jurnal Ilmiah Galuh Justisi*, *8*(2), 168. https://doi.org/10.25157/justisi.v8i2.3479

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Qi Dong, J., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, *122*(July 2018), 889–901. https://doi.org/10.1016/j.jbusres.2019.09.022

Wicaksana, R. H., Imam Munandar, A., Samputra, P. L., Salemba, J., No, R., & Indonesia, J. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic. *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi*, *22*(2), 143–158. Retrieved from http://dx.doi.org/10.33164/iptekkom.22.2.2020.143-158

Widyawati. (2021). Data Pengguna e-HAC Tidak Bocor. *Kementerian Kesehatan*. Retrieved from https://sehatnegeriku.kemkes.go.id/baca/rilis-media/20210901/2538410/data-pengguna-e-hac-tidak-bocor/

Yuninda, S. P., Pasma, S. A., & Mantoro, T. (2022). Patient Data Security in Telemedicine Services from Data Misuse in Health Practice. *2022 IEEE 8th International Conference on Computing, Engineering and Design, ICCED 2022*. https://doi.org/10.1109/ICCED56140.2022.10010685

Zaoui, F., & Souissi, N. (2020). Roadmap for digital transformation: A literature review. *Procedia Computer Science*, *175*, 621–628. https://doi.org/10.1016/j.procs.2020.07.090