Triwikrama: Jurnal Ilmu Sosial
Volume 8 No. 4 Tahun 2025
E-ISSN: 2988-1986
Open Access:

PERAN KEAMANAN SIBER DALAM MELINDUNGI DATA KESEHATAN: TANGGUNG JAWAB NEGARA DAN LEMBAGA INTERNASIONAL DALAM ERA DIGITAL

Nahlda Zahrani Balqish[1], Atika Puspita Marzaman[2]
[1,2]Departemen Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin, Makassar, Indonesia

ARTICLE INFO

Article history:
Received: May 2025
Revised: May 2025
Accepted: May 2025
Available online

Korespondensi: Email:
[1]naldazahra24@gmail.com,
[2]tika.marzaman@gmail.com

Abstrak

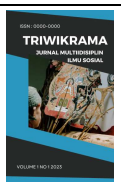
Perkembangan teknologi dalam sektor kesehatan telah membawa kemajuan dalam pengelolaan data medis, namun juga menambah resiko terhadap ancaman keamanan siber yang mengancam kerahasiaan data kesehatan. Ancaman tersebut, yang meliputi serangan siber, peretasan data, serta gangguan operasional seperti *malware* dan *ransomware*, memerlukan perlindungan data yang komprehensif, keamanan siber menjadi hal yang sangat penting untuk menjaga kerahasiaan data, mencegah kerugian finansial yang besar, serta menghindari kerusakan reputasi organisasi dan ancaman terhadap keselamatan pasien. Negara memiliki peran utama dalam menetapkan regulasi yang melindungi data kesehatan, membangun infrastruktur keamanan siber, serta meningkatkan kesadaran dan pelatihan bagi tenaga kesehatan. Di sisi lain, organisasi internasional seperti WHO, *Europol*, maupun INTERPOL berperan penting dalam menyusun standar global, memberikan pelatihan, dan memperkuat kerja sama antarnegara. Perlindungan data kesehatan membutuhkan pendekatan holistik yang melibatkan teknologi, hukum, etika, dan edukasi, serta kolaborasi lintas sektor antara pemerintah dan Lembaga global guna menciptakan sistem kesehatan yang aman dan terpercaya.

Kata kunci: Keamanan Siber, Data Kesehatan, Perlindungan data medis, WHO, Serangan Siber, Kolaborasi Internasional, Regulasi data kesehatan.

Abstract

Advances in technology in the healthcare sector have brought progress in medical data management, but they have also increased the risk of cyber threats that threaten the confidentiality of health data. These threats, which include cyber-attacks, data breaches, operational disruptions such as malware and ransomware, require comprehensive data protection, making cybersecurity essential to maintain data confidentiality, prevent significant financial losses, and avoid damage to organizational reputation and threats to patient safety. Governments play a key role in establishing regulations that protect health data, building cybersecurity infrastructure and increasing awareness training for healthcare for workers. On the other hand, international organization such as the WHO, Europol, and INTERPOL play an important role in developing global standards, providing training, and strengthening cooperation between countries. Health data protection requires a holistic approach that involves technology, law, ethics, and education, as well as cross-sector collaboration between governments and global institutions to create a safe and reliable healthcare system.

***Keywords**: Cybersecurity, Health Data, Medical Data Protection, WHO, Cyber Attacks, International Collaboration, Health Data Regulation.*



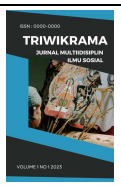
PENDAHULUAN

Perkembangan teknologi pada sektor kesehatan saat ini, secara signifikan sangat mempermudah pengelolaan data medis, namun juga meningkatkan resiko ancaman siber terhadap data kesehatan. Industri layanan kesehatan adalah target utama serangan siber karena informasi kesehatan pasien menjadi target utama yang dicari oleh para penjahat digital (Abbasi & Smith, 2024). Data tersebut adalah hal yang sangat sensitif sehingga diperlukan perlindungan yang kuat untuk menghindari kebocoran atau pencurian informasi yang dapat merugikan individu maupun institusi kesehatan. Ancaman dari permasalahan ini muncul dalam berbagai bentuk, seperti contohnya serangan siber, peretasan data, dan juga gangguan operasional *malware* dan *ransomware*.

Keamanan siber menjadi hal yang penting untuk bisa melindungi data kesehatan agar tetap terjaga kerahasiaannya, selain itu serangan terhadap data tersebut bisa menyebabkan kerugian finansial yang sangat besar bagi penyedia layanan kesehatan (Komaragiri & Edward, 2022), dan merusak reputasi organisasi kesehatan serta mengancam keselamatan pasien. Dalam konteks perlindungan data kesehatan oleh keamanan siber, tidak hanya harus berfokus pada aspek teknologi, tetapi juga aspek kebijakan, hukum, maupun etika. Ancaman seperti ini termasuk dalam kategori ancaman keamanan non-tradisional, yang menjadi bagian dari isu keamanan manusia (*Human Security*) yang bukan hanya mengancam privasi tetapi juga dimanfaatkan secara tidak baik dalam konflik, diplomasi, maupun manipulasi lintas negara, sehingga membutuhkan keamanan informasi yang memadai. Menurut Aditya (2018), keamanan informasi merupakan upaya dalam mengamankan asset informasi terhadap ancaman yang bisa saja timbul, yang secara tidak langsung dapat menjamin dan mengurangi resiko-resiko yang ada (Ramadhani, 2018). Aditya menambahkan bahwa, pengelolaan resiko yang tepat dapat membantu mengurangi potensi ancaman tersebut terhadap data sensitif dan mendukung bagaimana keberlanjutan organisasi kesehatan dalam menjaga kepercayaan pasien. Pada tahun 2023 lebih dari 6 juta orang terkena dampak pelanggaran data perawatan kesehatan (Shan, 2023).

Negara memiliki peran dan tanggung jawab untuk membuat regulasi kebijakan terkait perlindungan data (Boyne, 2020). Di tengah meningkatnya konektivitas digital yang pesat, perlindungan data kesehatan membutuhkan kolaborasi internasional dengan menerapkan kebijakan lintas negara dan adopsi standar global untuk menjamin keamanan yang setara. Organisasi kesehatan seperti WHO (*World Health Organization*) juga perlu ikut serta memastikan bahwa mereka mempunyai sistem yang andal dalam melindungi data kesehatan global. Tetapi kenyataannya saat ini masih banyak negara yang belum kuat sistem perlindungan datanya, regulasi seperti HIPAA (*Health Insurance Portability and Accountability Act*) di Amerika Serikat memberikan pedoman yang jelas mengenai bagaimana data kesehatan tersebut dikelola dan dilindungi dengan baik (Shah, 2023). Namun demikian, sering kali penerapannya terhambat oleh beberapa faktor, salah satunya adalah ketidakcukupan sumber daya dan infrastruktur yang dimiliki oleh organisasi kesehatan untuk mendukung kebijakan tersebut. Tidak banyak rumah sakit maupun fasilitas kesehatan memiliki anggaran dan keahlian yang cukup untuk mengimplementasikan sistem perlindungan data yang memadai.

Menurut penelitian yang dilakukan pada tahun 2020 oleh O'Brien dkk, sebagian besar organisasi perawatan kesehatan telah menetapkan praktik keamanan siber, Tingkat kesadaran dan pendidikan mengenai keamanan siber secara umum masih rendah (O'Brien *et al.*, 2020). Bahkan di negara-negara dengan regulasi yang ketat, tingkat kepatuhan terhadap regulasi ini masih beragam, dan banyak yang belum memenuhi standar minimum keamanan data yang



ditetapkan. Selain itu di beberapa negara berkembang, yang tantangannya lebih besar karena terbatasnya akses teknologi dan pengembangan sistem keamanan data yang canggih.

Pentingnya Pendidikan dan pelatihan bagi tenaga medis dan manajer data kesehatan juga menjadi bagian solusi. Pada artikel yang diterbitkan oleh *Journal of Medical System* (2020), organisasi kesehatan perlu melibatkan seluruh staf dalam program pelatihan perlindungan data secara berkelanjutan. Penguatan sumber daya manusia dalam hal keamanan data tidak hanya penting bagi pengamanan informasi pasien, tetapi juga untuk meningkatkan kepercayaan masyarakat terhadap sistem kesehatan itu sendiri. Tulisan ini bertujuan untuk menganalisis sejauh mana peran negara dan organisasi kesehatan dalam menjamin keamanan data kesehatan di era digital, dan bagaimana tantangan strategis yang dihadapi dalam mengimplementasikan kebijakan perlindungan data.

METODE PENELITIAN

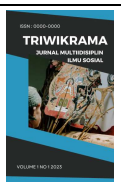
Penelitian ini menggunakan pendekatan kualitatif dengan metode studi pustaka (*Library Research*) yang bertujuan untuk menganalisis peran negara dan organisasi kesehatan dalam menjamin keamanan data kesehatan di era digital. Metode studi Pustaka adalah teknik pengumpulan data atau informasi yang relevan dengan topik penelitian dengan menggunakan dokumen-dokumen (Ainu Ningrum, 2022). Data dalam penelitian ini bersumber dari berbagai literatur sekunder yang relevan, termasuk jurnal ilmiah, regulasi internasional seperti HIPAA dan GDPR, laporan dari lembaga kesehatan dunia (WHO), serta dokumen resmi kebijakan dan kasus pelanggaran data kesehatan. Penelusuran dilakukan secara sistematis melalui *database* akademik seperti *Google Scholar, ScienceDirect*, dan *ProQuest*.

Teknik analisis data yang digunakan adalah analisis isi (*content analysis*), dengan mengidentifikasi tema-tema kunci terkait keamanan siber, perlindungan data kesehatan, serta tantangan kebijakan nasional dan internasional. Untuk menjamin validitas data, dilakukan triangulasi sumber dengan membandingkan berbagai dokumen dari lembaga yang kredibel. Hasil analisis diharapkan dapat memberikan pemahaman yang mendalam terkait strategi perlindungan data kesehatan, serta kontribusi aktor negara dan organisasi kesehatan dalam memperkuat sistem keamanan informasi di sektor kesehatan.

HASIL DAN PEMBAHASAN

A. Peran Negara Dalam Perlindungan Data Kesehatan

Setelah memahami bagaimana pentingnya perlindungan data Kesehatan dan berbagai macam ancaman yang dapat terjadi, negara memiliki peran dalam menetapkan regulasi yang melindungi data Kesehatan. Negara tetap berkewajiban untuk mengatur serta mengawasi implementasi kebijakan maupun standar yang harus diikuti oleh penyedia layanan Kesehatan untuk memastikan data pasien terlindungi dengan baik. Bukan hanya sebuah regulasi, tetapi harus memuat bentuk nyata pembuatan undang-undang, agar menyediakan sanksi yang berlaku ketika pelanggaran terjadi. Pada contoh kasus yang ada di Amerika Serikat, *Health Insurance Portability and Accountability Act* (HIPAA) menetapkan peraturan *security role* semenjak tahun 2005 (Abbasi & Smith, 2024) dan telah menetapkan standar keamanan nasional yang mengharuskan penyedia layanan kesehatan menerapkan pengamanan administratif, fisik, dan teknis terhadap data elektronik pasien. Penegakan aturan tersebut dilakukan oleh otoritas negara *Health and Human Services Office for Civil Rights* (HHS OCR) yang bisa menyelidiki kepatuhan dan memberikan sanksi berupa denda perdata yang signifikan hingga menyentuh angka USD 50.000 per insiden pelanggaran. Tahun 2025 ini WHO Eropa mengeluarkan laporan



mengenai *General Data Protection Regulation* (GDPR) dalam mensyaratkan enkripsi dan tata kelola privasi yang ketat terhadap data kesehatan pribadi (WHO *European Region*, 2025).

Secara umum, negara-negara memperkuat standar keamanan melalui regulasi serta menyediakan mekanisme pengawasan dan sanksi untuk mengurangi resiko kebocoran data pasien. Namun, meskipun regulasi dan mekanisme telah diterapkan, kenyataannya ancaman siber masih terus berkembang. Seperti yang tercatat dalam laporan *The U.S. Department of Health and Human Services* (HHS), pada tahun 2023, terdapat lebih dari 548 insiden kebocoran data dan dilaporkan ke *Office of Civil Rights* (OCR) dan data ini mempengaruhi hampir 122 juta individu *(U.S. Department of Health and Human Services Office for Civil Rights*, 2023). Negara-negara lain juga mengalami hal yang serupa, sebagai contoh Irlandia pada tahun 2021 terjadi serangan *ransomware* terhadap sistem rumah sakit yang menyebabkan gangguan layanan Kesehatan untuk jutaan pasien. Serangannya menyebabkan kebocoran data pribadi dan medis, dan mengganggu operasi rumah sakit selama beberapa minggu (Mashinchi *et al.*, 2024). Di Indonesia ancaman serupa juga terjadi, pada tahun 2021, data pribadi peserta BPJS Kesehatan sebanyak 279 juta orang bocor dan dijual di forum *hacker* (Satria Nusantara *et al.*, 2024). Data yang bocor mencakup informasi sensitif seperti Nomor Induk Kependudukan (NIK), nama lengkap, dan berbagai macam data diri masyarakat. Hal ini menegaskan bahwa, sistem Kesehatan sangat rentan dalam permasalahan keamanan siber dan merugikan banyak pihak.

Setelah mengidentifikasi permasalahan tersebut beberapa tantangan dalam perlindungan data Kesehatan untuk negara adalah sebagai berikut:

a. Masalah Kebijakan

   Jika dilihat dan dianalisis lebih jauh salah satu tantangan yang paling signifikan dalam permasalahan ini adalah masih banyak negara tidak memiliki kebijakan yang kuat untuk menjamin keamanan dan pengelolaan data Kesehatan yang tepat (Oktaviana R. *et al.*, 2024). Kesenjangan ini menyebabkan kerentanan dalam perlindungan data maupun privasi khususnya dalam era digital ini yang semuanya serba terhubung. Kebijakan yang dibuat terkadang tidak mengikuti perkembangan teknologi yang pesat dan penegakan hukum masih lemah, sehingga banyak penyedia layanan Kesehatan tidak mematuhi standar keamanan yang telah ditetapkan.

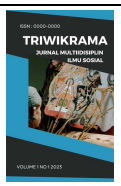
b. Masalah Manajemen Data

   Manajemen data diperlukan untuk mengatur bagaimana strategi yang efektif dalam mengatasi kondisi rentan dalam keamanan (Yeboah-Ofori *et al.*, 2024). Beberapa tantangannya meliputi kualitas data yang buruk sehingga menyebabkan Kesimpulan dan Keputusan yang salah, kedua adalah kesalahan dalam memberikan akses terhadap data tersebut. Ketika terdapat kesalahan pengelolaan hak akses, dapat mengakibatkan pengaksesan yang tidak sah dan pelanggaran data. Dan yang ketiga adalah sistem yang digunakan untuk menyimpan data pasien tidak dilengkapi dengan pengamanan yang memadai, seperti enkripsi atau kontrol akses yang tepat, yang membuat data lebih gampang untuk dicuri dan disalahgunakan.

Sehingga untuk mengatasi tantangan-tantangan ini, beberapa Langkah dapat diambil oleh negara untuk memperkuat perlindungan data Kesehatan:

1. Penguatan Infrastruktur Keamanan Siber

   Negara perlu mendorong penyediaan layanan Kesehatan untuk memperbarui infrastruktur TI, audit keamanan rutin, pembaruan perangkat lunak secara berkala, serta pelatihan keamanan siber bagi staf pelayanan kesehatan mereka (Aldosari, 2025). Investasi dalam perangkat keras maupun lunak. Infrastruktur yang lebih modern akan sangat membantu mengurangi kerentanannya terhadap serangan seperti *ransomware*, *phising*,



malware. Selain itu dalam pemantauan dan deteksi ancaman, pelayanan Kesehatan perlu menerapkan sistem pemantauan untuk mendeteksi aktivitas yang mencurigakan dalam jaringan mereka. Sistem deteksi intrusi (IDS) atau Sistem Pencegahan Intrusi (IPS) dapat sangat membantu mendeteksi serangan lebih awal dan mencegah kerusakan yang lebih besar

2. Pelatihan dan Sertifikasi Keamanan Siber

   Negara perlu memastikan bahwa tenaga medis dan staf administratif disektor Kesehatan mendapatkan pelatihan yang memadai tentang keamanan siber. Pelatihan ini tidak hanya mencakup pengenalan ancaman siber tetapi juga langkah-langkah praktis untuk melindungi data pasien. Bukan hanya itu, mereka memerlukan simulasi dan pemahaman mengenai bagaimana sistem tersebut berjalan, untuk melatih meningkatkan respons kemampuan mereka dalam menangani insiden.

3. Kerja Sama Internasional Untuk Mengatasi Ancaman Siber

   Perlindungan data Kesehatan adalah tantangan global, sehingga negara harus meningkatkan kolaborasi Internasional dengan Lembaga seperti WHO, *Europol*, dan negara lain dalam berbagai informasi terkait ancaman siber dan cara-cara mitigasinya. Dalam kolaborasinya terdapat pertukaran teknologi keamanan, sumber daya, dan data intelijen mengenai serangan yang sering terjadi. Negara dapat saling mendukung dalam menangani ancaman siber yang berpotensi mengganggu sistem Kesehatan secara global. Selain itu, hal ini juga membantu untuk meningkatkan kesadaran internasional yang mendorong negara-negara untuk menerapkan kebijakan yang lebih ketat dan efektif.

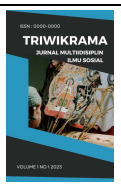
4. Peningkatan Pengawasan dan Penegakan Hukum

   Negara harus memperkuat mekanisme pengawasan dan mempercepat proses penegakan hukum terhadap pelanggaran data Kesehatan. Selain itu, meningkatkan transparansi mengenai pelanggaran dan sanksi yang dijatuhkan dapat meningkatkan kepercayaan publik terhadap sistem Kesehatan, ini dapat menjadi sinyal ataupun tanda kepada publik bahwa negara serius dalam melindungi data pribadi mereka.

B. Peran Lembaga Internasional Dalam Keamanan Data Kesehatan

Lembaga Internasional, khususnya *World Health Organization* (WHO) memegang peran penting sebagai koordinator dan pembina kebijakan global dalam perlindungan data Kesehatan. WHO, Bersama dengan Lembaga internasional lainnya, bertugas untuk merumuskan pedoman dan standar keamanan yang diterapkan di sektor Kesehatan secara global. Melalui kebijakan dan regulasi yang dikeluarkan, WHO membantu negara-negara mengembangkan sistem yang aman dan dapat diandalkan untuk melindungi data Kesehatan. WHO secara aktif mengeluarkan pedoman untuk keamanan data kesehatan dan teknologi digital (Labrique *et al.*, 2020). WHO Eropa telah merilis panduan kesiapan keamanan siber pada sektor yang menegaskan bahwa serangan siber pada rumah sakit dan sistem kesehatan dapat mengancam akses layanan vital dan menargetkan kelompok rentan. Dokumen WHO memaparkan kerangka penilaian kesiapan keamanan berdasarkan tiga pilar utama, seperti aksesibilitas, privasi (melalui enkripsi dan anonimisasi data), serta tata kelola sistem kesehatan digital.

- Aksesibilitas: Memastikan bahwa layanan Kesehatan tetap dapat diakses tanpa gangguan, meskipun ada ancaman terhadap sistem
- Privasi: Perlindungan data pribadi pasien melalui enkripsi dan anonimisasi data, untuk memastikan bahwa informasi pasien hanya dapat diakses oleh pihak berwenang.
- Tata Kelola Sistem Kesehatan Digital: Mengelola sistem ataupun platform digital secara transparan dan aman, dengan memastikan bahwa kebijakan yang ada dapat memitigasi ancaman yang berkembang.

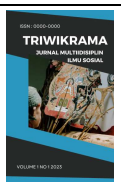


Selain itu, rencana aksi kesehatan digital WHO (2023-2030) di Kawasan Eropa menekankan keamanan dan privasi data dengan fokus pada peningkatan kesadaran dan teknologi perlindungan data (WHO *European Region*, 2025). Kebijakan WHO seperti yang di implementasikan WHO Eropa tersebut bertujuan untuk meningkatkan kepercayaan publik dan integritas sistem kesehatan digital.

WHO menegaskan bahwa keamanan siber di sektor kesehatan merupakan persoalan keamanan nasional. Selain itu, pelanggaran data dapat mengganggu aspek kemanusiaan karena serangan siber yang berhasil berpotensi menimbulkan resiko langsung pada kehidupan pasien. Kebocoran data kesehatan melanggar hak privasi individu dan perlahan mengikis kepercayaan publik terhadap sistem kesehatan(Tin *et al*., 2023). Implikasi ini menegaskan perlunya pendekatan holistik yang mempertimbangkan hak privasi dan keselamatan publik dalam kebijakan keamanan dan kesehatan. Temuan ini menegaskan pentingnya kolaborasi lintas-sektoral antara pemerintah, organisasi internasional, dan penyedia layanan kesehatan untuk menghadapi kompleksitas ancaman siber di sektor kesehatan. Setiap sektor bekerja sama dalam mengidentifikasi, mencegah, dan merespons serangan siber dengan cara yang terintegrasi, efektif, dan terkoordinasi. Pada tahun 2024 kemarin, *Europol* yang merupakan Badan Penegakan Hukum Uni Eropa merilis laporan *Internet Organised Crime Threat Assessment* (IOCTA) yang menyoroti tren ancaman siber yang berkembang, termasuk serangan terhadap sektor Kesehatan (IOCTA, 2024). Laporan ini memberikan penilaian strategis mengenai ancaman yang dihadapi oleh sektor Kesehatan dan memberikan rekomendasi untuk meningkatkan ketahanan terhadap serangan siber. *Europol* ini juga bekerja sama dengan negara-negara anggota untuk meningkatkan kapasitas mereka dalam menghadapi ancaman siber melalui pelatihan dan berbagai intelijen.

Lembaga internasional memiliki peran penting dalam kolaborasi global untuk meningkatkan ketahanan sistem Kesehatan. Dengan mengembangkan kebijakan dan program yang berfokus pada keamanan data Kesehatan, Lembaga ini bukan hanya membimbing negara-negara dalam memperkuat segi infrastruktur, tetapi turut mengharmonisasikan upaya-upaya internasional dalam melawan ancaman siber. Kerja sama lintas sektoral antara pemerintah, organisasi internasional, dan penyedia layanan kesehatan sangat penting untuk mencapai keberhasilan dalam menghadapi ancaman siber yang sangat dinamis. Selain program yang dijalankan oleh WHO dan *Europol*, ternyata terdapat beberapa upaya lembaga internasional lain dalam menghadapi ancaman ini, seperti *Cybercrime Programme* yang dijalankan oleh *International Criminal Police Organization* atau biasa disebut INTERPOL dimana tujuannya untuk mengkoordinasikan upaya antar negara-negara untuk melawan kejahatan dunia digital yang menargetkan sektor kesehatan. Program lainnya termasuk pelatihan keamanan siber, dan membuat platform untuk berbagai informasi tentangan ancaman siber dan bagaimana teknik peretasan terbaru yang dapat membahayakan data Kesehatan. Adapun program-program lembaga yang lainnya seperti ISO/IEC 27001 dari *International Organization for Standarization* yang menetapkan standar untuk sistem manajemen keamanan informasi termasuk dalam sektor Kesehatan, lalu ada *Global Programme on Cybercrime* oleh *United Nations* yang membantu negara-negara meningkatkan kemampuannya menghadapi ancaman siber. UN menyediakan pelatihan untuk tenaga profesional di sektor publik dan swasta, termasuk juga Kesehatan.

Dengan membangun kerja sama yang kuat antara pemerintah, organisasi internasional, dan penyedia layanan Kesehatan, akan sangat membantu dalam menciptakan perlindungan data Kesehatan yang lebih baik. Melalui penerapan standar global, pelatihan yang berkelanjutan, serta berbagi informasi dan teknologi, lembaga internasional berperan sebagai pilar utama



dalam menciptakan sistem Kesehatan yang aman, transparan, dan dapat diandalkan, yang pada akhirnya akan melindungi hak privasi, individu dan keselamatan pasien di seluruh dunia.

SIMPULAN

Di era digital saat ini, perlindungan data kesehatan menjadi isu strategi dan mendesak yang memerlukan perhatian serius dari berbagai pihak, terutama negara dan organisasi kesehatan internasional. Meskipun kemajuan teknologi telah memudahkan pengelolaan data medis, hal ini juga meningkatkan resiko serangan siber yang dapat menyebabkan kebocoran informasi sensitif, merugikan institusi Kesehatan, serta mengancam keselamatan dan privasi pasien. Negara memiliki tanggung jawab utama dalam membentuk kebijakan, regulasi, dan mekanisme penegakan hukum yang efektif untuk menjamin keamanan data kesehatan. Tantangan besar yang dihadapi negara meliputi, lemahnya kebijakan, kurangnya infrastruktur keamanan siber, serta rendahnya kesadaran dan pelatihan di kalangan tenaga Kesehatan. Oleh karena itu, diperlukan penguatan sistem melalui Pembangunan infrastruktur TI yang kuat, pelatihan berkala, kerja sama internasional, dan pengawasan yang ketat.

Lembaga internasional seperti WHO, *Europol*, INTERPOL, dan UN juga memainkan peran sentral sebagai koordinator, penyusun standar global, serta penyedia bantuan teknis dan pelatihan. Pendekatan lintas sektor dan kolaboratif antara negara, organisasi internasional dan penyedia layanan Kesehatan sangat diperlukan untuk mengatasi yang semakin kompleks. Secara keseluruhan, keberhasilan perlindungan data Kesehatan memerlukan *holistic* yang tidak hanya mencakup aspek teknologi, tetapi juga aspek hukum, kebijakan, etika, dan pendidikan. Sinergi antara aktor lokal dan global akan sangat menentukan terciptanya sistem Kesehatan digital yang aman, andal, dan dapat dipercaya oleh publik.

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 Knowledge Learning and Science Technology ISSN: 2959-6386 (Online)*, *3*(3), 278–287. https://doi.org/10.60087/jklst.vol3.n3.p.278-287

Ainu Ningrum, N. (2022). “Strategi Pembelajaran pada Anak Berkebutuhan Khusus dalam Pendidikan Inklusi”. *Indonesian Journal of Humanities and Social Sciences*, *3*(2), 181–196. https://doi.org/10.33367/ijhass.v3i2.3099

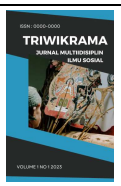
Aldosari, B. (2025). “Cybersecurity in Healthcare: New Threat to Patient Safety”. *Cureus*. https://doi.org/10.7759/cureus.83614

Boyne, S. M. (2020). "Data Protection in the United States: U.S. National Report” (pp. 409–455). https://doi.org/10.1007/978-3-030-28049-9_17

IOCTA. (2024, July 26). *Internet Organised Crime Threat Assessment (IOCTA) 2024*. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024?utm_source=chatgpt.com

Komaragiri, V. B., & Edward, A. (2022). “AI-Enhanced Information Security: Safeguarding Government and Healthcare PHI”. *International Journal of Engineering and Computer Science*, *11*(08), 25601–25617. https://doi.org/10.18535/ijecs/v11i08.4697

Labrique, A., Agarwal, S., Tamrat, T., & Mehl, G. (2020). “WHO Digital Health Guidelines: a milestone for global health”. *Npj Digital Medicine*, *3*(1), 120. https://doi.org/10.1038/s41746-020-00330-2



Mashinchi, M. I., Acton, T., & Datta, P. M. (2024). "When healthcare becomes sick: Recovering from ransomware". *Journal of Information Technology Teaching Cases*. https://doi.org/10.1177/20438869241279443

O'Brien, N., Martin, G., Grass, E., Durkin, M., Darzi, A., & Ghafur, S. (2020). "Cybersecurity in Healthcare: Comparing Cybersecurity Maturity and Experiences Across Global Healthcare Organizations". *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3688885

Oktaviana R., S., Handayani, P. W., & Hidayanto, A. N. (2024). "Health organization challenges in health data governance implementation: A systematic review". *Journal of Infrastructure, Policy and Development*, *8*(6), 3892. https://doi.org/10.24294/jipd.v8i6.3892

Ramadhani, A. (2018). "KEAMANAN INFORMASI". *Nusantara - Journal of Information and Library Studies*, *1*(1), 39. https://doi.org/10.30999/n-jils.v1i1.249

Satria Nusantara, A. H., Kahirul Umam, I., & Lubis, M. (2024). "Jaminan Informasi dan Keamanan yang Lebih Baik: Studi Kasus BPJS Kesehatan". *NUANSA INFORMATIKA*, *18*(2), 120–127. https://doi.org/10.25134/ilkom.v18i2.202

Shah, W. F. (2023). "Preserving Privacy and Security: A Comparative Study of Health Data Regulations - GDPR vs. HIPAA". *International Journal for Research in Applied Science and Engineering Technology*, *11*(8), 2189–2199. https://doi.org/10.22214/ijraset.2023.55551

Shan, M. (2023). "Real-Time Monitoring of Health Security Attacks with R-based Data Visualization Dashboard". *Proceedings of the 14th ACM International Conference on Bioinformatics, Computational Biology, and Health Informatics*, 1–1. https://doi.org/10.1145/3584371.3613035

Tin, D., Hata, R., Granholm, F., Ciottone, R. G., Staynings, R., & Ciottone, G. R. (2023). "Cyberthreats: A primer for healthcare professionals". *The American Journal of Emergency Medicine*, *68*, 179–185. https://doi.org/10.1016/j.ajem.2023.04.001

U.S. Department of Health and Human Services Office for Civil Rights. (2023). *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

WHO European Region. (2025, March 26). "WHO/Europe launches guide to strengthen cybersecurity in digital health". *WHO European Region*.

Yeboah-Ofori, A., Jafar, A., Abisogun, T., Hilton, I., Oseni, W., & Musa, A. (2024). "Data Security and Governance in Multi-Cloud Computing Environment". *2024 11th International Conference on Future Internet of Things and Cloud (FiCloud)*, 215–222. https://doi.org/10.1109/FiCloud62933.2024.00040