Volume 5 Issue 2 (2025) Pages 1133-1145

Amkop Management Accounting Review (AMAR)

ISSN: 2828-2248 (Online)

A Systematic Analysis of Telemedicine Behavior, Compliance and Cyber Resilience In Indonesia

Ade Indra Jaya ✉, **Sumeidi Kadarisman**[2], **Raden Ricky Agusiady**[3]

✉,2,3 *Universitas Sangga Buana YPKP Bandung, Indonesia*

Abstract

Indonesia's digital health push has fostered an integrated telemedicine ecosystem centered on SATUSEHAT Mobile and major private platforms, intensifying cross-system clinical data exchange. This raises the salience of three dimensions: behavior (human factors), compliance (regulatory/standards alignment), and cyber resilience (prevent, respond, and recover). This study maps the evidence on these dimensions in Indonesia's telemedicine context and develops a maturity evaluation model with baseline operational practices. We conducted a Systematic Literature Review guided by PRISMA, covering publications from 2020 to 2025 in major scholarly databases under inclusion criteria specific to Indonesian telemedicine. Eligible studies were extracted and analyzed qualitatively using NVivo, with open axial selective coding, to produce a thematic synthesis and a concept map across the three focal dimensions. The synthesis yields four theme clusters: (1) behavior & security literacy (credential hygiene, social engineering awareness, BYOD/remote access); (2) audit & operational compliance (logging/audit trails, breach reporting, adoption of standards/certifications); and (3) incident response & resilience (runbooks, backup/restore, failover, BCP/DRP testing). Key gaps include consent traceability across FHIR-based interoperability flows, end-to-end resilience indicators (e.g., integration MTTR, standardized failover tests), and comparative cross-platform assessments. Outputs comprise a behavior→compliance→resilience conceptual model, a maturity evaluation framework, and non-policy baseline operational practices.

Keywords: *Telemedicine; User Behavior; Data Compliance; Cyber Resilience; SATUSEHAT Mobile.*

✉ Corresponding author :
Email Address: ade.indrajaya@gmail.com

INTRODUCTION

Over the past five years, Indonesia's healthcare ecosystem has undergone a rapid digital transformation. The implementation of electronic medical records, teleconsultation services, e-prescriptions, and cross-facility data integration signifies the nation's accelerated shift toward digital health infrastructure. The transition of *PeduliLindungi* into *SATUSEHAT Mobile* in March 2023 represents a strategic move by the government to develop a comprehensive citizen health application, shifting its focus from pandemic tracing to general health management. Systemically, this digital evolution is grounded in the Health Law No. 17 of 2023, which establishes the National Health Information System as the foundation for interoperability through the SATUSEHAT (IHS) platform based on the FHIR framework. In the private sector, telemedicine platforms such as Halodoc and Alodokter have pioneered integrated digital healthcare services, offering online consultations, digital pharmacies, and home laboratory testing. However, this wave of digitalization has heightened concerns over data privacy, cybersecurity, and systemic resilience—issues that now stand at the forefront of healthcare digital transformation.

As healthcare systems become increasingly digitized, cybersecurity risks have grown correspondingly. Indonesia has faced several major cyber incidents, including the ransomware attack on the National Data Center in June 2024, which disrupted various government digital services, including healthcare-related services. This incident underscores the critical importance of robust governance and cybersecurity resilience. In response, the Indonesian government enacted the Personal Data Protection Law (PDP), effective in October 2024, which mandates data controllers and processors to implement strict security measures, report data breaches, and comply with legal sanctions. In the context of telemedicine, where sensitive medical data are collected and processed across multiple entities, these regulations are particularly crucial to maintaining patient trust and ensuring lawful data protection.

Globally, the healthcare sector has become a primary target of cyberattacks. Reports from WHO (2024) and Interpol (2023) indicate a sharp rise in cyber incidents targeting hospitals and healthcare institutions across Southeast Asia, including Indonesia. Threats such as phishing, ransomware, and large-scale data breaches have resulted in patient data leaks, service disruptions, and significant financial losses. Although Indonesia has established several legal frameworks, such as the Electronic Information and Transactions Law (Law No. 11 of 2008), Government Regulation No. 71 of 2019 on Electronic Systems and Transactions, and Ministry of Health Regulation No. 1171 of 2011 on Hospital Information Systems, their effectiveness in ensuring cybersecurity compliance across healthcare facilities remains uncertain. Many hospitals still face challenges in legal literacy, resource limitations, and insufficient regulatory enforcement.

Previous studies have emphasized that human factors are often the weakest link in cybersecurity. Uhrle (2024) found that human behavior — including weak password practices, limited awareness of phishing threats, and noncompliance with institutional policies — plays a significant role in security failures. Similarly, Yeng *et al.,* (2022) observed that in entirely paperless hospitals, medical staff often feel overwhelmed by stringent cybersecurity protocols, leading some to bypass them for convenience. Supporting this, Sari *et al.,* (2022) discovered a significant gap between management-level cybersecurity policies and their actual implementation among hospital personnel.

Given these challenges, this study aims to analyze cybersecurity behavior in Indonesian healthcare facilities by pursuing three main objectives: (1) to identify factors influencing cybersecurity behavior in hospital environments; (2) to evaluate the level of compliance with existing cybersecurity policies; and (3) to examine the strategies of cyber resilience adopted by healthcare institutions. The research seeks to contribute theoretically by enhancing behavioral models of cybersecurity compliance and practically by offering insights for policymakers and healthcare administrators to strengthen information security management in the healthcare sector.

This study aims to provide a comprehensive understanding of cybersecurity dynamics in Indonesia's healthcare industry through an empirical and systematic approach. Moreover, it seeks to develop an adaptive framework to anticipate emerging digital threats. The findings are expected to inform evidence-based policymaking for national health data protection, foster a culture of cybersecurity awareness among healthcare professionals, and enhance public trust in digitally driven healthcare systems.

Hypothesis

Empirical studies by Irwandy *et al.,* (2024) and Rosyad *et al.,* (2024) highlight that cybersecurity behavior is strongly associated with individual characteristics, including age, educational background, and previous exposure to cybersecurity training. Younger healthcare professionals and those with higher levels of digital literacy tend to demonstrate better adaptive behavior toward technological safeguards and data protection protocols. Conversely, limited digital competence among older practitioners often correlates with greater vulnerability to phishing or social engineering attacks. Furthermore, structured training programs enhance employees' risk perception and improve adherence to secure digital practices. Therefore, demographic attributes and continuous cybersecurity awareness education are critical determinants in shaping responsible digital behavior among telemedicine practitioners in Indonesia's evolving healthcare ecosystem.

H1: *Cybersecurity behavior among healthcare professionals in telemedicine services in Indonesia is significantly influenced by demographic factors (such as age and education level) and prior cybersecurity training.*

Drawing on findings from Yeng *et al.,* (2022), compliance behavior in cybersecurity is driven by individuals' perceived capability to follow established procedures (self-efficacy), their belief in the benefits of compliance (perceived usefulness), and the transparency and coherence of the policies themselves. When healthcare workers perceive that cybersecurity rules are practical, clearly communicated, and directly related to their daily workflow, they are more likely to internalize and consistently implement them. Conversely, ambiguous or overly technical policies tend to reduce motivation and increase the likelihood of procedural neglect. Moreover, self-efficacy serves as a mediating factor, reinforcing confidence in applying security standards, especially when employees are adequately trained and supported by leadership. Hence, fostering clarity in policy design and promoting confidence in execution are essential for achieving sustainable compliance within telemedicine institutions.

H2: *Compliance with cybersecurity policies is significantly determined by self-efficacy, perceived usefulness, and the clarity of information security policies within healthcare organizations.*

According to Hasegawa *et al.,* (2024), organizational resilience is achieved through the cohesive integration of technological infrastructure, human capability, and governance mechanisms. In developing nations like Indonesia, the readiness to detect, respond to, and recover from cyber incidents depends not only on advanced tools but also on human adaptability and institutional coherence. A well-integrated system enables early anomaly detection, streamlined incident communication, and rapid post-attack recovery. Human resources trained in digital forensics, policy enforcement, and system continuity planning play a vital role in maintaining operational stability. Institutional frameworks that mandate proactive risk management and regular security audits further enhance this resilience. Thus, resilience emerges as a multidimensional construct that requires synchronized efforts between technology, people, and organizational policy to ensure the sustainability of telemedicine systems in a volatile digital landscape.

H3: *Cybersecurity resilience in telemedicine organizations is positively influenced by the integration of technology, human resources, and institutional policies.*

The interrelationship among behavior, compliance, and resilience reflects a socio-technical perspective on cybersecurity, in which human actions and organizational systems interact dynamically. When healthcare professionals exhibit strong cybersecurity behaviors, such as using secure authentication, recognizing phishing attempts, and safeguarding patient data, these individual practices directly contribute to organizational robustness. Simultaneously, adherence to institutional security policies ensures consistency, accountability, and coordinated responses across the telemedicine network. Together, these factors form a reinforcing loop: improved awareness leads to higher compliance, and higher compliance, in turn, strengthens systemic resilience by minimizing vulnerabilities and optimizing recovery processes. This holistic relationship suggests that developing a security-oriented culture and embedding compliance values within organizational norms are essential to achieving sustainable cyber resilience in Indonesia's telemedicine sector.

H4: *Cybersecurity behavior and compliance with security policies collectively and positively affect the overall level of cybersecurity resilience within telemedicine systems.*

METHODOLOGY

This study employs a Systematic Literature Review (SLR) design guided by the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework to ensure methodological rigor and transparency. The population of this study comprises peer-reviewed publications on cybersecurity behavior, compliance, and resilience within the context of telemedicine in Indonesia, published between 2020 and 2025 across reputable academic databases such as Scopus, ScienceDirect, PubMed, and SpringerLink. Articles were selected through defined inclusion and exclusion criteria, focusing on empirical and conceptual studies relevant to Indonesia's telemedicine ecosystem.

Data were collected through a systematic search, screening, and eligibility assessment, followed by the extraction of key findings and metadata. Qualitative data analysis was conducted using NVivo 14 software, employing open, axial, and selective coding to develop thematic syntheses and relational maps across the three primary dimensions: cybersecurity behavior, compliance, and resilience. The researcher's role was interpretive, focusing on identifying conceptual linkages and underlying patterns across studies while ensuring validity through triangulation of sources, peer debriefing, and audit-trail documentation. The analytical procedure enabled the construction of an integrative thematic framework that captures the dynamic interrelationships among human, organizational, and regulatory aspects of cyber resilience in Indonesian telemedicine.

RESULT & DISCUSSION

Results

An analysis of 15 scientific articles on cybersecurity in the context of digital health systems in Indonesia and globally was conducted. Three main categories were identified through the coding process: Cybersecurity Behaviour, Regulatory Compliance, and Cybersecurity System Resilience. Each category consists of several subthemes that illustrate the complexity of the issues and potential solutions.

The reviewed articles were published between 2020 and 2025, indicating an increase in research interest, particularly after the COVID-19 pandemic, which accelerated the adoption of telemedicine (Wijaya, 2022). The distribution of publications is shown in Appendix 10, which presents Indonesian telemedicine studies by year of publication (2020–2025) and illustrates a significant upward trend in 2024–2025. Methodologically, there are variations: qualitative studies (legal analysis, case studies), quantitative studies (surveys), systematic literature reviews (SLRs), and mixed-methods studies. A summary of this study is presented in Appendix 3, in the Indonesian Telemedicine Article Extraction table (15 studies).

Source Triangulation

The researcher used source triangulation by combining 15 national and international journal articles that covered various aspects of cybersecurity in digital health systems. These ranged from regulatory studies (Swartz *et al.*,, 2022) and national security reports (BSSN, 2023) to privacy ethics research (Ordonez, 2020). Comparing different viewpoints gave a well-rounded thematic understanding. Urban studies mostly discussed user behavior and service quality, while rural research focused on infrastructure gaps and security risks, echoing the WHO (2021) findings on digital inequality. Altogether, this mix of sources revealed consistent global issues while highlighting local gaps, particularly weak consumer protection in Indonesia, thereby boosting the study's external validity.

Table 1. Result of Source Tringulation

Theme	Percentage	Key Focus in Literature	Supporting Theory / Framework	Interpretation
Compliance	42.3%	Emphasizes regulations, audits, certifications, and consumer protection in telemedicine.	Compliance Theory (Tyler, 1990) highlights the importance of legal legitimacy in enhancing compliance among users and service providers.	The dominance of this theme shows that regulatory issues are the primary concern in current research on telemedicine.
Cyber Resilience	34.6%	Focuses on data breaches, weak incident response, and the need for national security standards.	Cyber Resilience Framework (Linkov *et al.*, 2018) – explains the need to strengthen Indonesia's digital health defense systems.	This theme reflects growing awareness of cybersecurity gaps and the urgent need for stronger data protection frameworks.
Behavior	23.1%	Highlights user adoption, digital literacy, and trust in telemedicine platforms.	Technology Acceptance Model (TAM) (Davis, 1989) and UTAUT2 (Venkatesh *et al.*, 2012) indicate that usage intention is influenced by performance expectancy and habit.	Although less frequent, this theme remains crucial for understanding user interaction and acceptance of digital health technologies.

Methode Tringulation

In method triangulation, researchers do not rely on a single analytical technique; instead, they combine diverse methods to explore and interpret data. Thematic analysis was conducted using NVivo software and supported by visualisations, including word clouds, treemaps, and matrix coding, which provided an overview of the thematic distribution across articles. This strategy strengthens the consistency and sharpness of the analysis because each finding can be confirmed through mutually reinforcing cross-methods. In this qualitative study, method triangulation was applied to ensure the analysis was not dependent on a single approach and was confirmed through complementary analytical techniques.

Table 2. Result of Method Tringulation

Theme	Frequency (Number of Mentions)	Key Focus	Interpretation
Cyber Resilience	9	Emphasizes system readiness, risk management, and data encryption as key aspects of digital health defense.	Represents the most dominant theme, highlighting technical preparedness and the need for stronger system protection.
Compliance	11	Focuses on data privacy, legal adherence, and regulatory enforcement in telemedicine.	Ranked second in prominence, indicating strong scholarly attention to governance and legal frameworks.
Cybersecurity Behavior	6	Relates to user awareness, digital literacy, and responsible security practices among healthcare personnel and patients.	Though less frequent, it underscores the behavioral dimension that is crucial to sustaining secure digital health ecosystems.

Triangulation of Theory

To strengthen the validity of NVivo-based thematic analysis, this study employed theoretical triangulation to interpret data through multiple conceptual lenses, linking themes and subthemes with established theories in technology, behavior, and regulation. The Technology Acceptance Model (TAM) (Davis, 1989) explains that technology adoption behavior is shaped by perceived usefulness and ease of use, clarifying how users engage with digital security practices in healthcare. The Theory of Planned Behavior (TPB) (Ajzen, 1991) further contextualizes cybersecurity behavior, emphasizing that positive attitudes toward security may not translate into action without institutional norms or technical support.

From a technical standpoint, the DeLone and McLean IS Success Model (2003) assesses cyber resilience through system quality, information quality, user satisfaction, and organizational impact. Meanwhile, the Protection Motivation Theory (PMT) (Rogers, 1975) elucidates protective actions driven by threat perception and self-efficacy, relevant to secure user behavior and institutional responses to cyber threats. Lastly, Regulatory Compliance Theory (Parker, 2002) underscores the role of legal frameworks, supervision, and governance in promoting adherence to data protection and e-health regulations. Integrating these theories provides a comprehensive understanding of cybersecurity dynamics in digital health, where each framework contributes distinct explanatory power to the network of identified themes.

Table 3. Result of Theory Tringulation

Theory / Framework	Author(s) / Year	Core Concept	Relevance to Research Themes
Technology Acceptance Model (TAM)	Davis (1989)	Technology adoption is influenced by perceived usefulness and ease of use.	Explains user behavior and adoption of digital security practices in healthcare systems.
Theory of Planned Behavior (TPB)	Ajzen (1991)	Attitude, subjective norms, and perceived behavioral control shape intention to act.	Interprets cybersecurity behavior, showing that attitudes alone do not ensure secure actions without institutional support.
DeLone and McLean IS Success Model	DeLone & McLean (2003)	System success depends on system quality, information quality, user satisfaction, and organizational impact.	Provides a framework for analyzing Cyber Resilience, focusing on system performance and technical reliability.
Protection Motivation Theory (PMT)	Rogers (1975)	Protective behavior arises from threat appraisal and coping appraisal (self-efficacy and response efficacy).	Explains secure user behavior and institutional responses to cyber threats in digital health contexts.
Regulatory Compliance Theory	Parker (2002)	Legal structures, regulatory oversight, and organizational accountability drive compliance.	Supports the Compliance theme by linking policy adherence with governance and data protection standards.

Discussion

Cybersecurity Behavior

This subtheme encompasses three critical issues: user awareness, responses to cyber threats, and risky digital habits. Several studies reveal that cybersecurity awareness among healthcare workers remains low. Pratama *et al.,* (2024) reported that the level of digital literacy among medical personnel remains inadequate to detect phishing and malware threats, while Alfi *et al.,* (2023) noted that most healthcare workers have not received formal digital security training. Common risky behaviors, such as password sharing and storing medical data on personal devices, further expose vulnerabilities. As Kadarisman *et al.,* (2020) emphasized, human resources are the primary drivers of organizational operations, responsible for controlling and effectively utilizing other resources. Behavioral issues also relate to adoption factors, digital literacy, and patient trust in telemedicine services. Tri Aji and Ramadani (2024) identified low digital literacy as a significant barrier to telemedicine adoption, whereas Mizan (2023) highlighted the importance of trust in the use of applications. The NVivo Word Cloud (Appendix 4) highlights dominant terms such as trust, literacy, and behavior, reinforcing findings from global empirical studies that identify digital literacy as a key determinant of telehealth adoption (Alshahrani *et al.*, 2022).

Regulatory Compliance

The literature reveals a clear gap between existing regulations and practical implementation in the field. Swartz *et al.*, (2022) observed that the Personal Data Protection Law (UU PDP) has not yet become the primary reference in developing digital health information systems, while Mutiah *et al.*, (2025) criticized that Government Regulation No. 47/2021 lacks detailed technical guidance for healthcare providers. From an ethical perspective, Ordonez (2020) emphasized the need to integrate bioethical principles into the design of telemedicine systems. Compliance emerges as the dominant theme, encompassing data protection (UU PDP), health regulations, and the need for robust security audits. Damasus (2024) noted the weak implementation of the PDP Law, while Bonsapia (2025) stressed the need to harmonize it with the Health Law. Similarly, Safira (2025) and Ramadhan (2025) proposed ISO 27001 certification to strengthen digital governance. The cross-article Heatmap Matrix (Appendix 5) visualizes the prevalence of compliance issues, aligning with international studies that underscore the role of data protection standards such as HIPAA and GDPR in fostering public trust (Bouri & Ravi, 2021).

Cyber Resilience

Cyber resilience is a recurring theme in many studies, emphasizing preparedness and adaptive capacity in the face of digital threats. Hassan *et al.*, (2024) revealed that only a few hospitals have established and regularly tested disaster recovery systems. According to BSSN (2023), over 403 million anomalous traffic incidents were recorded in Indonesia's health sector during 2023. Ordonez (2020) further identified the vulnerability of Internet of Medical Things (IoMT) devices as a common entry point for attacks. Key issues related to resilience include the BPJS data breach (Sorisa, 2024), infrastructure challenges in rural regions (Mutiah, 2025), and weak incident response mechanisms. Literature analysis also revealed that Indonesia still lacks a health-sector-specific CERT, unlike developed countries. The Evidence Bubble Map (Appendix 13) illustrates the dominance of resilience issues in private telemedicine platforms such as Halodoc and Alodokter. These findings align with those of Linkov *et al.*, (2018), who emphasize the importance of preventive, absorbent, recovery, and adaptive mechanisms to ensure sustainable cybersecurity in digital public services.

DOI: 10.37531/amar.v5i2.3278

CONCLUSION

Based on the systematic literature review of 15 selected articles on user behavior, regulatory compliance, and cyber resilience in Indonesian telemedicine, analyzed using NVivo-assisted thematic analysis, several key conclusions can be drawn. The findings indicate that telemedicine adoption in Indonesia is significantly influenced by digital literacy, perceived ease of use, trust in healthcare providers, and sociocultural factors. User behavior is highly contextual and shaped by subjective norms, consistent with the Theory of Planned Behavior (Ajzen, 1991), while trust and perceived security align with the Technology Acceptance Model (Davis, 1989) and UTAUT2 (Venkatesh *et al.,*, 2012). The main barriers include low digital security literacy and the absence of longitudinal post-pandemic studies, both of which could threaten long-term sustainability. In terms of regulation, compliance with the Personal Data Protection Law (UU PDP) remains inconsistent due to weak oversight and the lack of independent audits. Legal legitimacy, as described by Tyler (1990), plays a crucial role in fostering public trust and institutional adherence. Cyber resilience also remains a significant challenge, with many organizations inadequately prepared for cyberattacks, particularly in rural areas. The literature highlights the need for a dedicated healthcare CERT, standardized incident response mechanisms, and regular security testing, aligning with the Cyber Resilience Framework (Linkov *et al.,*, 2018).

Overall, this study concludes that telemedicine in Indonesia should be viewed as a multidimensional system requiring simultaneous attention to behavioral, regulatory, and resilience aspects. The application of theoretical, data, and methodological triangulation enhances the validity of these findings, integrating perspectives from behavioral theories (TAM, UTAUT2), compliance frameworks, and cyber resilience models to build a comprehensive understanding of digital health security. Strengthening policy integration, digital literacy, and technological infrastructure is essential for advancing sustainable, secure, and trustworthy telemedicine practices across Indonesia's healthcare ecosystem.

REFERENCES

A. Yi, M. Al-Emran, and K. Shaalan, "Theories in Cybersecurity Behavior Studies," MDPI Applied Sciences, vol. 13, no. 9, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/9/5700/pdf

Agusiady, R., Dwiputrianti, S., Kusumastuti, D., Sedarmayanti. (2021). Mewujudkan Good Corporate Governance – Tata Kelola Perushaan yang Baik, Di Era Industri 4.0 dan Masyarakat 5.0. ISBN: 978-623-02-3324-1. Deepublish Publisher.

Agusiady, R., Sedarmayanti, Sunarsi, D., Mulyani. S., R. (2022). Manajemen Rumah Sakit. ISBN: 978-623-02-5066-8. Deepublish Publisher.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. Applied Sciences, 13(9), 5700. https://www.mdpi.com/2076-3417/13/9/5700

Alodokter. Kebijakan Privasi (Privasi). Alodokter

Ameen, A. H., & Mohammed, M. A. (2023). Dimensions of artificial intelligence techniques, blockchain, and cybersecurity in the Internet of Medical Things: Opportunities, Challenges, and Future Directions. *Journal of Intelligent Systems*, 32(3), 567–589. https://doi.org/10.1515/jisys-2022-0267

American Psychological Association. (2017). *Ethical principles of psychologists and code of conduct*. https://www.apa.org/ethics/code

Antara. (2023, 27 Februari). Kemenkes: Aplikasi PeduliLindungi jadi SatuSehat Mobile mulai 1 Maret. Antara News

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., & Flury, R. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 20*(1), 146. https://doi.org/10.1186/s12911-020-01161-7

ASIS International. (2024, 26. Juni). Indonesia Refuses to Pay $8M Ransom in Data Center Cyberattack (insiden PDN). ASIS International

AWS. (2025). Halodoc: Optimizing Resource Use for 20% Improvement on AWS Graviton3 (studi kasus). Amazon Web Services, Inc.

Azwar, A. R., & Sirait, E. S. (2025). The legal framework for personal data protection amidst hospital competition. *Proceedings of ICOSEND 2025*. https://www.atlantis-press.com/article/126008670.pdf

Bazeley, P., & Jackson, K. (2013). Qualitative Data Analysis with NVivo (2nd ed.). SAGE Publications.

Boell, S. K., & Cecez-Kecmanovic, D. (2015). On being 'systematic' in literature reviews. Information Systems Journal, 25(4), 613–635. https://doi.org/10.1016/j.is.2014.07.001

Booth, A., Sutton, A., & Papaioannou, D. (2016). Systematic approaches to a successful literature review (2nd ed.). Sage.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage Publications.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems, 19*(4), 9–30. https://doi.org/10.1080/07421222.2003.11045748

Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess thematic saturation. PLOS ONE, 15(5), e0232076.

Haleem, A., Javaid, M., Singh, R. P., & Suman, R. (2021). Telemedicine for healthcare: Capabilities, features, barriers, and applications. Sensors International, 2, 100117. https://doi.org/10.1016/j.sintl.2021.100117

Halodoc Blog. (2024, 6 September). How Halodoc Achieved ISO/IEC 27701:2019 Certification. Halodoc Blog

Health Sector Coordinating Council. (2023). Health Industry Cybersecurity – Securing Telehealth and Telemedicine (HIC-STAT). healthsectorcouncil.org

Hernandez-Jaimes, M. L., & Martinez-Cruz, A. (2023). Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets, and Cloud–Fog–Edge architectures. *Journal of Biomedical Informatics*, 136, 104206. https://www.sciencedirect.com/science/article/pii/S254266052300210X

Irwandy, I., Suharti, N., & Fadillah, R. (2024). Cybersecurity culture among healthcare workers in Indonesia. *Research Square*. https://www.researchsquare.com/article/rs-5421169/latest.pdf

ISO/IEC 27001:2013 - Information Security Management Systems. ISO/IEC 27001:2022 - Information security management systems

Jain, S., Ashok, P., & Prabhu, S. (2024). Emerging Technologies for Cybersecurity in Healthcare: Evaluating Risks and Implementing Standards. *IEEE Xplore*. https://ieeexplore.ieee.org/abstract/document/10803219/

Jannink, K. J. B. (2025). How do the protection motivation theory and the self-determination theory influence healthcare employees' intention to perform safe cyber behaviour? http://essay.utwente.nl/105210/

JBI. (2020). JBI manual for evidence synthesis. Scoping Reviews - Resources | JBI

K. Hasegawa, N. O'Brien, and M. Prendergast, "Cybersecurity Interventions in Health Care Organizations in Low-and Middle-Income Countries: Scoping Review," JMIR, vol. 26, no. 1, 2024. [Online]. Available: https://www.jmir.org/2024/1/e47311/

Kruse, C. S., Karem, P., Shifflett, K., Vegi, L., Ravi, K., & Brooks, M. (2017). Evaluating barriers to adopting telemedicine worldwide: A systematic review. Journal of Telemedicine and Telecare, 24(1), 4–12. https://doi.org/10.1177/1357633X16674087

Kadarisman, S. dkk. (2020). The Impact of Human Resource Management Implementation in Business Strategy in Creating Sustainable Competitive Advantage. Proceedings of the 2nd Annual Conference on Blended Learning, Educational Technology and Innovation (ACBLETI 2020). https://www.atlantis-press.com/proceedings/acbleti-20/125957860

Linkov, I., Trump, B. D., Keisler, J. M., & Collier, Z. A. (2018). Resilience and risk: Methods and application in environment, cyber, and social domains. Risk Analysis, 38(9), 1834–1845. https://doi.org/10.1111/risa.12991

Liu, X. (2024). Data ownership in the AI-powered integrated health care. JMIR Medical Informatics, 12, e57754.

Makarim, E. (2024). Telemedicine in the legal system in Indonesia. Dialogia Iuridica, 16(1).

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). Qualitative Data Analysis: A Methods Sourcebook (3rd ed.). SAGE Publications.

Monteiro, A. C. B., França, R. P., Arthur, R., & Iano, Y. (2021). An overview of the medical Internet of Things, artificial intelligence, and cloud computing employed in health care from a modern panorama. In *Healthcare Technology* (pp. xx–xx). Springer. https://link.springer.com/chapter/10.1007/978-3-030-75220-0_1

OECD. (2020). Digital security and data protection in health: Building resilience and trust. OECD Publishing. https://doi.org/10.1787/9789264812003-en

Ordonez, A. (2020). Cybersecurity in the healthcare industry (Honors thesis). DePauw University.

P. K. Sari *et al.*,, "Information security behavior in health information systems: a review," Healthcare, vol. 10, no. 12, 2022. [Online]. Available: https://www.mdpi.com/2227-9032/10/12/2531

P. K. Yeng, M. A. Fauzi, and B. Yang, "Human factors in cybersecurity compliance in paperless hospitals," MDPI Info, vol. 13, no. 7, 2022. [Online]. Available: https://www.mdpi.com/2078-2489/13/7/335

Page, M. J., *et al.*, (2021). PRISMA 2020 statement. PLOS Medicine, 18(3), e1003583.

Parker, C. (2002). *The open corporation: Effective self-regulation and democracy*. Cambridge University Press. https://doi.org/10.1017/CBO9780511495194

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114.

Roobini, S., Kavitha, M., & Sujaritha, M. (2022). Cybersecurity threats to IoMT-enabled healthcare systems. In *Cybersecurity in IoMT* (pp. xx–xx). Taylor & Francis. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003256243-6

Salas, J. A., *et al.*, (2022). Guarding the digital health data as the front gate. Journal of Legal, Ethical & Regulatory Issues, 24(S4), 47–60.

Saleh & Winata (2023). Indonesia's Cyber Security Strategy: Problems and Challenges – IJCAH Proceedings.

Snigdha *et al.*,, 2025. Cybersecurity in Healthcare IT Systems: Business Risk Management and Data Privacy Strategies – TAJET Journal.

Snyder, H. (2019). Literature reviews as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Suci, R. P., & Dhamanti, I. (2024). Cybersecurity dalam sistem informasi rumah sakit Indonesia. *Journal Innovative*. https://j-innovative.org/index.php/Innovative/article/download/12632/8537

Sudarsana, I. P., & Ramli, K. (2023). Information security risk assessment using factor analysis of information risk (FAIR) in the healthcare sector: Scoping review. Jurnal Darma Agung, 31(4). https://jurnal.darmaagung.ac.id/index.php/jurnaluda/article/download/3236/3198

Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the Internet of Medical Things. *Clinical Therapeutics*, 43(1), 1–10. https://www.sciencedirect.com/science/article/pii/S2211883721000721

Torraco, R. J. (2016). Writing integrative literature reviews: Using the past and present to explore the future. *Human Resource Development Review, 15*(4), 404–428. https://doi.org/10.1177/1534484316671606

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, *14*(3), 207–222. https://doi.org/10.1111/1467-8551.00375

Tyler, T. R. (1990). Why do people obey the law? Yale University Press.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Wong, G., Greenhalgh, T., Westhorp, G., *et al.*, (2013). RAMESES publication standards: Realist syntheses. *BMC Medicine, 11*(1), 21. https://doi.org/10.1186/1741-7015-11-21

World Health Organization (WHO). (2021). Global strategy on digital health 2020–2025. World Health Organization. https://apps.who.int/iris/handle/10665/344249

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research, 39*(1), 93–112. https://doi.org/10.1177/0739456X17723971

Yeng, P. K., *et al.*, (2022). Assessing the legal aspects of information security requirements for health care in 3 countries. *JMIR Human Factors, 9*(2). https://humanfactors.jmir.org/2022/2/e30050/

Yeng, P. K., Fauzi, M. A., & Yang, B. (2022). A comprehensive assessment of human factors in relation to cybersecurity compliance of healthcare staff in a paperless hospital. Preprints. https://www.academia.edu/download/89549893/preprints202203.0247.v1.pdf

Yuliaty, F. (2017). Employee Empowering Through Information Technology And Creativity In Organizations. International Journal Of Economic Perspectives. 11. 54–59.