Reconfiguring Healthcare Cybersecurity: Zero-Trust Architectures, Legacy Medical Devices, And The Socio-Technical Implications Of Windows 11 Adoption In Clinical Environments

[1] Dr. Alexander M. Havel
[1] Faculty of Engineering and Information Technology, University of Melbourne, Australia

Received: 28th Nov 2025 | Received Revised Version: 20th Dec 2025 | Accepted: 03th Jan 2026 | Published: 21th Jan 2026

Volume 08 Issue 01 2026

Abstract

The accelerating digitization of healthcare delivery has intensified long-standing cybersecurity vulnerabilities rooted in legacy medical devices, fragmented network architectures, and historically perimeter-centric security paradigms. Healthcare organizations increasingly rely on interconnected clinical workstations, electronic health records, artificial intelligence-driven diagnostics, and networked medical devices that were not designed for modern threat landscapes. This study develops a comprehensive, theoretically grounded analysis of zero-trust security adoption in healthcare, with a particular focus on the operational, governance, and socio-technical implications of upgrading hospital clinical workstations to Windows 11 environments. Anchored in recent empirical and conceptual scholarship, the article interrogates how zero-trust principles intersect with legacy systems, regulatory accountability, and emerging AI-enabled clinical workflows. Central to this inquiry is the evaluation of Windows 11 as a security modernization vector within hospital infrastructures, drawing on recent evaluative research that examines compatibility constraints, security controls, and workflow disruptions associated with contemporary operating system adoption in clinical contexts (Nayeem, 2026).

The study employs a qualitative, interpretive research design grounded in systematic literature synthesis, governance analysis, and conceptual modeling. Rather than treating zero trust as a purely technical framework, the article situates it within broader debates on organizational learning, institutional trust, ethical accountability, and cyber risk management in healthcare. The analysis demonstrates that while zero-trust architectures promise granular access control, continuous authentication, and reduced lateral movement, their effectiveness is fundamentally constrained by legacy medical devices that cannot natively support modern cryptographic standards or identity-centric security models (Gellert et al., 2023). The transition to Windows 11 clinical workstations is shown to function as both a catalyst and a stress test for zero-trust implementation, exposing tensions between security hardening and clinical usability, as well as between regulatory compliance and operational resilience (Nayeem, 2026).

Findings suggest that zero-trust adoption in healthcare must be understood as a socio-technical transformation rather than a discrete technological upgrade. The article argues that Windows 11 adoption, when aligned with zero-trust principles, can enhance baseline security postures through hardware-backed security, secure boot mechanisms, and identity integration, yet simultaneously exacerbates interoperability challenges with legacy devices and vendor-locked ecosystems (Eastwood, 2024). The discussion advances a multi-layered framework for healthcare cybersecurity governance that integrates zero trust, AI accountability, blockchain-based integrity mechanisms, and legacy system risk mitigation. By synthesizing diverse strands of cybersecurity, health informatics, and governance literature, this article contributes a theoretically expansive and policy-relevant perspective on the future of secure healthcare digital transformation.

Keywords: Zero-trust architecture; healthcare cybersecurity; legacy medical devices; Windows 11 clinical workstations; digital health governance; AI security.

Cite This Article: Dr. Alexander M. Havel. (2026). Reconfiguring Healthcare Cybersecurity: Zero-Trust Architectures, Legacy Medical Devices, And The Socio-Technical Implications Of Windows 11 Adoption In Clinical Environments. The American Journal of Management and Economics Innovations, 8(01), 26–33. Retrieved from https://www.theamericanjournals.com/index.php/tajmei/article/view/7295

1. Introduction

Healthcare systems have historically occupied a paradoxical position within the broader landscape of information security: they manage some of the most sensitive and consequential data in modern society, yet they often rely on technological infrastructures characterized by obsolescence, fragmentation, and underinvestment in cybersecurity modernization (Burrell, 2024). The rapid expansion of digital health technologies, including electronic health records, networked diagnostic tools, and artificial intelligence-driven clinical decision support systems, has dramatically increased the attack surface of healthcare organizations while simultaneously raising the stakes of cyber incidents (Help Net Security, 2023). High-profile cyberattacks, most notably the WannaCry incident that disrupted the United Kingdom's National Health Service, have underscored the systemic risks associated with legacy operating systems and perimeter-based security models in healthcare environments (Department of Health, 2018). Although this attack occurred years ago, its underlying lessons regarding outdated systems and insufficient segmentation remain acutely relevant across global healthcare systems (Khan MJ, 2023).

At the conceptual core of contemporary cybersecurity discourse is the growing recognition that traditional perimeter security models are fundamentally misaligned with the realities of modern, highly distributed, and interconnected digital ecosystems (Northcutt, 2005). Perimeter-centric approaches assume a trusted internal network and an untrusted external environment, an assumption that collapses under conditions of cloud computing, remote access, mobile devices, and third-party integrations that now define healthcare IT infrastructures (He et al., 2022). Zero-trust architecture emerges within this context as both a critique of legacy security paradigms and a normative vision for continuous verification, least-privilege access, and identity-centric control (Tyler & Viana, 2021). In healthcare, zero trust has been framed not merely as a technical solution but as a strategic reorientation of trust relationships among users, devices, applications, and data flows (Gellert et al., 2023).

Despite the conceptual appeal of zero-trust models, their practical implementation in healthcare remains deeply contested and uneven (Ghasemshirazi et al., 2023). Hospitals and clinical organizations operate within complex socio-technical environments where security controls must coexist with time-critical workflows, safety-critical devices, and regulatory obligations that prioritize patient outcomes over infrastructural experimentation (Habli et al., 2020). Legacy medical devices, many of which run outdated operating systems or proprietary firmware, represent a particularly intractable challenge. These devices are often mission-critical, difficult to patch, and tightly coupled with clinical processes, making their replacement or isolation both costly and operationally risky (Eastwood, 2024). Industry analyses indicate that a significant proportion of healthcare providers continue to rely on medical equipment running unsupported or end-of-life operating systems, thereby constraining the feasibility of zero-trust enforcement at the device level (Kaspersky, 2024).

Within this contested landscape, operating system modernization has emerged as a focal point of cybersecurity strategy, particularly in relation to hospital clinical workstations that serve as primary interfaces between clinicians and digital systems. Recent evaluative research has examined the adoption of Windows 11 in hospital environments as a potential bridge between zero-trust security principles and entrenched legacy infrastructures (Nayeem, 2026). This work highlights both the security enhancements embedded in modern operating systems, such as hardware-based root of trust and enhanced identity management, and the compatibility challenges that arise when these systems interact with legacy medical devices and specialized clinical software (Nayeem, 2026). The significance of this analysis lies not only in its technical findings but also in its implicit challenge to deterministic narratives of security modernization that overlook organizational, ethical, and governance dimensions.

The existing literature on healthcare cybersecurity tends to fragment along disciplinary lines, with technical analyses of zero-trust architectures rarely engaging deeply with clinical workflow realities, and governance-oriented studies often abstracting away from the material constraints of legacy systems (Shojaei et al., 2024). Studies on artificial intelligence in healthcare security further complicate this picture by introducing questions of algorithmic accountability, explainability, and trust that intersect with, but are not reducible to, network security considerations (Markus et al., 2021). Blockchain-based proposals for securing healthcare data and AI pipelines add yet another layer of complexity, promising tamper resistance and auditability while raising concerns about scalability and integration with existing systems (Kasralikar et al., 2025).

This article addresses a critical gap in the literature by offering an integrative, theoretically expansive analysis of zero-trust adoption in healthcare that foregrounds the role of operating system modernization, specifically Windows 11 clinical workstations, as a socio-technical intervention. Rather than evaluating zero trust or Windows 11 adoption in isolation, the study examines their interaction within the broader ecology of legacy medical devices, regulatory accountability, and organizational learning. Drawing on recent scholarship that evaluates Windows 11 deployment in clinical settings (Nayeem, 2026), the article situates technical findings within a wider analytical framework that encompasses risk governance, ethical responsibility, and institutional trust.

The central research problem guiding this study is the tension between the normative promise of zero-trust security architectures and the empirical realities of healthcare IT environments characterized by legacy dependencies and constrained modernization pathways. While zero trust is frequently presented as an inevitable or necessary evolution of cybersecurity practice, its translation into healthcare contexts raises unresolved questions about feasibility, proportionality, and unintended consequences (Burrell, 2024). The adoption of Windows 11 in hospital clinical workstations exemplifies this tension, functioning simultaneously as a security upgrade and as a disruptive force that can destabilize established workflows and device ecosystems (Nayeem, 2026).

By engaging deeply with these issues, this article seeks to contribute to scholarly debates on healthcare cybersecurity in three primary ways. First, it provides a historically informed and theoretically grounded account of zero-trust architectures as they relate to healthcare delivery organizations, moving beyond purely technical descriptions (Gellert et al., 2023). Second, it critically examines operating system modernization as a governance and risk management strategy, using Windows 11 adoption as a focal case informed by recent evaluative research (Nayeem, 2026). Third, it advances a multi-dimensional framework for future research and policy that integrates zero trust, AI accountability, and legacy system management within a coherent conceptual model. In doing so, the article responds to calls for more holistic and context-sensitive approaches to healthcare cybersecurity research (Debnath, 2023).

2. Methodology

The methodological approach adopted in this study is qualitative, interpretive, and integrative, reflecting the complex and multi-layered nature of healthcare cybersecurity as both a technical and socio-organizational phenomenon (Hong et al., 2018). Rather than seeking to generate new empirical data through experimentation or surveys, the study synthesizes and critically interprets existing scholarly, policy, and industry literature to construct a theoretically rich analysis of zero-trust adoption and operating system modernization in healthcare contexts (Page et al., 2021). This approach is particularly appropriate given the ethical, safety-critical, and infrastructural constraints that limit experimental interventions in live clinical environments (Habli et al., 2020).

The literature corpus underpinning this analysis was assembled through purposive sampling of peer-reviewed journal articles, systematic reviews, policy reports, and authoritative industry analyses focusing on zero-trust architectures, healthcare cybersecurity, legacy systems, artificial intelligence security, and operating system modernization. Particular attention was given to recent studies that explicitly address healthcare delivery organizations and clinical environments, ensuring contextual relevance (Gellert et al., 2023). The evaluative study of Windows 11 adoption in hospital clinical workstations serves as a conceptual anchor for the analysis, providing a concrete instantiation of broader theoretical and governance issues (Nayeem, 2026).

Analytically, the study employs a thematic synthesis strategy that identifies recurring conceptual tensions, assumptions, and normative claims across the literature. Themes such as trust reconfiguration, legacy system inertia, risk governance, and usability-security trade-offs were iteratively developed through close reading and comparative analysis of sources (Shojaei et al., 2024). This process was informed by established qualitative appraisal frameworks to ensure methodological rigor and transparency, particularly in assessing the relevance and credibility of diverse sources (Hong et al., 2018).

A key methodological decision in this study is the explicit rejection of technological determinism. Rather than treating zero-trust architectures or Windows 11 adoption as inherently beneficial or inevitable, the analysis situates these interventions within specific organizational, regulatory, and ethical contexts (Burrell, 2024). This stance allows for a more nuanced examination of counter-arguments and unintended consequences, including the risk that security modernization efforts may exacerbate inequalities between well-resourced and under-resourced healthcare organizations (Debnath, 2023).

The study also incorporates a governance-oriented analytical lens, drawing on risk management and accountability literature to assess how zero-trust adoption reshapes responsibility for cybersecurity failures and patient harm (Habli et al., 2020). This lens is particularly relevant in healthcare, where cybersecurity incidents can have direct implications for patient safety and clinical outcomes (Help Net Security, 2023). By integrating governance analysis with technical considerations, the methodology supports a holistic interpretation of cybersecurity transformation.

Limitations of this methodological approach must be acknowledged. The reliance on secondary sources means that findings are contingent on the quality and scope of existing literature, which itself may reflect publication biases or regional emphases (Page et al., 2021). Additionally, while the evaluative study of Windows 11 adoption provides valuable insights, its findings may not be universally generalizable across all healthcare contexts, particularly in low-resource settings with different infrastructural constraints (Nayeem, 2026). Nevertheless, the interpretive depth afforded by this approach enables a level of theoretical integration and critical reflection that would be difficult to achieve through narrowly empirical methods alone (He et al., 2022).

3. Results

The results of this integrative analysis emerge not as numerical outputs or statistically bounded findings, but as interpretive insights derived from systematic engagement with the literature on healthcare cybersecurity, zero-trust architectures, and operating system modernization. In line with qualitative and theoretical traditions in information systems research, the results are presented as thematically structured outcomes that illuminate patterns, tensions, and emergent dynamics across diverse scholarly and professional sources (Shojaei et al., 2024). Each interpretive result reflects a convergence of evidence rather than an isolated claim, and each is grounded in prior research to maintain analytical rigor (Page et al., 2021).

One of the most salient results is the identification of zero trust as an aspirational rather than fully realizable security state within contemporary healthcare environments. Across the literature, zero trust is consistently framed as a guiding philosophy emphasizing continuous verification, least-privilege access, and explicit trust boundaries (Tyler & Viana, 2021). However, when examined through the lens of real-world healthcare infrastructures, these principles encounter structural limitations imposed by legacy medical devices, vendor-specific constraints, and regulatory certification requirements that restrict rapid technological change (Eastwood, 2024). This finding aligns with broader critiques of zero trust as a conceptual ideal that must be pragmatically adapted rather than rigidly implemented (He et al., 2022).

A second key result concerns the role of clinical workstations as critical mediators between zero-trust frameworks and legacy ecosystems. The evaluative study of Windows 11 adoption in hospital clinical workstations demonstrates that modern operating systems can meaningfully enhance baseline security through features such as hardware-backed credential protection, secure boot processes, and deeper integration with identity and access management platforms (Nayeem, 2026). These features directly support zero-trust objectives by reducing implicit trust in devices and strengthening authentication mechanisms at the endpoint level. Yet, the same study highlights persistent compatibility challenges, particularly with older diagnostic peripherals and proprietary clinical applications that lack certification for newer operating systems (Nayeem, 2026). This duality positions clinical workstations as both enablers and bottlenecks in zero-trust transitions.

The analysis further reveals that legacy medical devices function as systemic risk multipliers rather than isolated vulnerabilities. Multiple sources emphasize that such devices are often embedded within clinical workflows in ways that preclude simple network isolation or replacement (Kaspersky, 2024; Burrell, 2024). When zero-trust policies are applied unevenly, securing modern endpoints while legacy devices remain implicitly trusted, the resulting security architecture may inadvertently concentrate risk rather than diffuse it. This finding challenges narratives that frame zero trust as inherently risk-reducing and underscores the importance of holistic threat modeling that accounts for heterogeneity across devices and systems (Ho et al., 2021).

Another interpretive result relates to the organizational and cultural dimensions of zero-trust adoption. The literature indicates that healthcare organizations frequently underestimate the degree to which zero trust requires changes in governance structures, decision-making authority, and professional norms (Gellert et al., 2023). Continuous authentication and granular access controls, while technically feasible, can be perceived by clinicians as intrusive or obstructive, particularly in high-pressure clinical contexts where speed and flexibility are paramount (Habli et al., 2020). The Windows 11 adoption analysis reinforces this point by documenting workflow disruptions and user resistance associated with stricter security enforcement, even when such enforcement aligns with best practices (Nayeem, 2026).

A further result concerns the intersection of zero trust with artificial intelligence and data-intensive healthcare applications. AI-driven diagnostic and administrative systems rely on large-scale data access and inter-system communication, potentially conflicting with zero-trust principles that emphasize strict segmentation and minimal access (Ajish, 2024). The literature suggests that without careful architectural design, zero-trust policies may inadvertently hinder AI system performance or exacerbate opacity in algorithmic decision-making (Markus et al., 2021). This tension is particularly pronounced in environments where AI applications coexist with legacy data repositories and heterogeneous device networks, reinforcing the need for adaptive rather than absolutist security strategies (Khan MM et al., 2025).

Collectively, these results depict a landscape in which zero trust and Windows 11 adoption offer meaningful security advancements but fall short of delivering comprehensive risk mitigation in isolation. The findings underscore the importance of viewing operating system modernization as one component of a broader socio-technical transformation that includes governance reform, legacy system management, and continuous organizational learning (Debnath, 2023).

4. Discussion

The findings presented above invite a deeper theoretical and critical examination of zero-trust architectures as instruments of transformation within healthcare cybersecurity. At a conceptual level, zero trust represents a fundamental reconfiguration of how trust is constructed, distributed, and enforced within digital systems (Khan MJ, 2023). Rather than assuming trust based on network location or institutional affiliation, zero trust operationalizes skepticism as a default stance, requiring continuous verification of identities, devices, and actions (He et al., 2022). In healthcare, this epistemic shift intersects with long-standing professional norms that emphasize interpersonal trust, clinical autonomy, and rapid decision-making under uncertainty (Habli et al., 2020).

The adoption of Windows 11 in hospital clinical workstations exemplifies the friction between these paradigms. On one hand, the security enhancements embedded in modern operating systems align closely with zero-trust principles by embedding trust anchors at the hardware and firmware levels (Nayeem, 2026). On the other hand, the operationalization of these controls within clinical workflows raises questions about proportionality and context sensitivity. Security mechanisms that introduce authentication delays or restrict access to clinical applications may be defensible from a risk management perspective, yet they can be perceived as undermining patient care when implemented without adequate consultation and adaptation (Gellert et al., 2023).

From a governance perspective, zero trust redistributes responsibility for cybersecurity failures in ways that are not yet fully reconciled within healthcare institutions. Traditional perimeter models often localized responsibility within IT departments, whereas zero trust implicates clinical staff, administrators, and even device vendors in maintaining security hygiene (Burrell, 2024). The Windows 11 evaluation highlights how operating system upgrades can shift accountability boundaries, particularly when legacy devices fail to meet new security baselines and require compensatory controls or workflow adjustments (Nayeem, 2026). This redistribution of responsibility raises ethical questions about fairness and professional burden, especially in resource-constrained healthcare settings (Debnath, 2023).

The persistence of legacy medical devices emerges as a central theoretical challenge to zero-trust orthodoxy. While zero trust presupposes the ability to authenticate and authorize every entity within a network, many legacy devices lack the computational capacity or software support to participate in such frameworks (Eastwood, 2024). Attempts to compensate through network segmentation or proxy controls may reduce exposure but do not eliminate implicit trust assumptions. This reality complicates claims that zero trust can fully replace perimeter security, suggesting instead that hybrid models may remain necessary for the foreseeable future (Ghasemshirazi et al., 2023).

The discussion also intersects with debates on artificial intelligence governance in healthcare. AI systems amplify both the benefits and risks of digital integration, requiring extensive data access while introducing new forms of opacity and vulnerability (Khan MM et al., 2025). Zero-trust principles, if applied rigidly, may constrain data flows in ways that hinder AI training and inference, yet insufficient controls risk data leakage and model manipulation (Ajish, 2024). The literature suggests that explainability and auditability, often proposed as ethical safeguards for AI, must be integrated with security architectures to ensure coherent governance (Markus et al., 2021). Blockchain-based proposals for securing AI pipelines illustrate this integrative ambition but also face scalability and interoperability challenges in legacy-laden healthcare environments (Kasralikar et al., 2025).

Another critical dimension concerns organizational learning and adaptability. Zero trust is frequently framed as a static architecture, yet the findings indicate that its effectiveness depends on continuous reassessment and iterative refinement (Tyler & Viana, 2021). The experience of Windows 11 adoption underscores the importance of feedback loops that incorporate clinician experiences, incident data, and evolving threat intelligence (Nayeem, 2026; Mandiant, 2022). Without such learning mechanisms, zero-trust implementations risk ossification, becoming misaligned with both technological change and clinical practice.

Limitations identified in this study warrant careful consideration. The reliance on secondary literature, while enabling broad theoretical synthesis, constrains the ability to capture granular organizational dynamics and regional variations (Page et al., 2021). Furthermore, much of the existing research reflects perspectives from high-income healthcare systems, potentially limiting applicability in low- and middle-income contexts where legacy dependencies may be even more pronounced (Debnath, 2023). These limitations point toward future research opportunities that combine ethnographic, longitudinal, and participatory methods to examine zero-trust adoption in situ.

Future research should also explore regulatory and procurement dimensions that shape cybersecurity trajectories. Certification processes for medical devices and operating systems often lag behind technological innovation, creating structural incentives for prolonged legacy use (Eastwood, 2024). Aligning regulatory frameworks with zero-trust principles, without compromising safety assurance, represents a complex but necessary policy challenge (Gellert et al., 2023). Additionally, comparative studies of different operating system strategies could illuminate alternative pathways to endpoint security beyond dominant vendor ecosystems (Nayeem, 2026).

5. Conclusion

This article has advanced a comprehensive, theoretically grounded examination of zero-trust security adoption in healthcare, foregrounding the role of legacy medical devices and the socio-technical implications of Windows 11 adoption in clinical workstations. By integrating diverse strands of cybersecurity, health informatics, and governance literature, the study demonstrates that zero trust should be understood not as a turnkey solution but as an evolving framework that must be adapted to the unique constraints and values of healthcare environments (Gellert et al., 2023).

The analysis underscores that operating system modernization, exemplified by Windows 11 deployment, can materially enhance endpoint security and support zero-trust objectives, yet it simultaneously exposes deep-seated incompatibilities within healthcare infrastructures (Nayeem, 2026). Legacy medical devices, organizational cultures, and regulatory regimes collectively shape the boundaries of feasible security transformation. Recognizing these interdependencies is essential for developing resilient, ethical, and clinically aligned cybersecurity strategies.

Ultimately, the future of healthcare cybersecurity lies not in the wholesale replacement of legacy systems or uncritical adoption of new paradigms, but in the cultivation of adaptive, learning-oriented governance frameworks that balance security, usability, and patient safety. Zero trust, when approached as a guiding philosophy rather than an absolute mandate, can contribute meaningfully to this balance, particularly when anchored in empirically informed analyses such as those examining real-world operating system adoption in clinical settings (Nayeem, 2026).

References

1. Kasralikar P, Polu OR, Chamarthi B, Veer Samara Sihman Bharattej Rupavath R, Patel S, Tumati R. Blockchain for securing AI-driven healthcare systems: a systematic review and future research perspectives. Cureus. 2025;17:e83136.
2. Nayeem M. Bridging zero-trust security and legacy medical devices: An evaluation of Windows 11 adoption in hospital clinical workstations. Frontiers in Emerging Artificial Intelligence and Machine Learning. 2026;3(1):1–8.
3. Burrell DN. Understanding healthcare cybersecurity risk management complexity. Land Forces Academy Review. 2024;29:38–49.
4. Gellert GA, et al. Zero trust and the future of cybersecurity in healthcare delivery organizations. Journal of Hospital Administration. 2023;12(1):1–8.
5. Northcutt S. Inside network perimeter security. 2nd ed. Sams; 2005.
6. Debnath S. Integrating information technology in healthcare: recent developments, challenges, and future prospects for urban and regional health. World Journal of Advanced Research and Reviews. 2023;19(1):455–463.
7. Kaspersky. Kaspersky finds 73% of healthcare providers use medical equipment with a legacy OS. 2024.
8. Tyler D, Viana T. Trust no one? A framework for assisting healthcare organisations in transitioning to a zero-trust network architecture. Applied Sciences. 2021;11(16):1–18.
9. Help Net Security. Rising cyber incidents challenge healthcare organizations. 2023.
10. Habli I, Lawton T, Porter Z. Artificial intelligence in health care: accountability and safety. Bulletin of the World Health Organization. 2020;98:251–256.
11. Khan MJ. Zero trust architecture: redefining network security paradigms in the digital age. World Journal of Advanced Research and Reviews. 2023;19(3):105–116.
12. He Y, et al. A survey on zero trust architecture: challenges and future trends. Wireless Communications and Mobile Computing. 2022;2022:1–13.
13. Eastwood B. Tips for health systems on managing legacy systems to strengthen security. HealthTech Magazine. 2024.
14. Ajish D. The significance of artificial intelligence in zero trust technologies: a comprehensive review. Journal of Electrical Systems and Information Technology. 2024;11:30.
15. Markus AF, Kors JA, Rijnbeek PR. The role of explainability in creating trustworthy artificial intelligence for health care: a comprehensive survey. Journal of Biomedical Informatics. 2021;113:103655.
16. Khan MM, Shah N, Shaikh N, Thabet A, Alrabayah T, Belkhair S. Towards secure and trusted AI in healthcare: a systematic review of emerging innovations and ethical challenges. International Journal of Medical Informatics. 2025;195:105780.
17. Ghasemshirazi S, Shirvani G, Alipour MA. Zero trust: applications, challenges, and opportunities. arXiv. 2023;1–23.
18. Ho G, et al. Hopper: modeling and detecting lateral movement (extended report). arXiv. 2021;1–20.
19. Mandiant. M-Trends 2022 special report: executive summary. 2022.
20. Shojaei P, Vlahu-Gjorgievska E, Chow YW. Security and privacy of technologies in health information systems: a systematic literature review. Computers. 2024;13(2):1–25.
21. Hong QN, Pluye P, Fàbregues S, et al. Mixed methods appraisal tool (MMAT), version 2018. BMJ. 2018;1–7.
22. Page MJ, McKenzie JE, Bossuyt PM, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ. 2021;372:n71.
23. Vijayasekhar D. Securing the future: strategies for modernizing legacy systems and enhancing cybersecurity. Journal of Artificial Intelligence and Cloud Computing. 2022;1(3):1–3.

24. Ofili BT, Erhabor EO, Obasuyi OT. Enhancing federal cloud security with AI: zero trust, threat intelligence, and compliance. World Journal of Research and Review. 2025;25:2377–2400.

25. Department of Health. Investigation: WannaCry cyber-attack on the NHS. UK National Audit Office. 2018.

26. International Conference on Communication Technologies (ComTech 2017). Institute of Electrical and Electronics Engineers; 2017.