pISSN:2349-5707 Volume:13, Issue 01, January-2026 eISSN:2349-5715

Zero-Trust Transformation in AI-Enabled Healthcare: Legacy Medical Devices, Clinical Workstations, and the Socio-Technical Reconfiguration of Cybersecurity Governance

Dr. Kairav Solen
Faculty of Science and Engineering, University of Groningen, The Netherlands

ABSTRACT: The accelerating digitization of healthcare infrastructures has intensified longstanding tensions between innovation, patient safety, and cybersecurity resilience. Hospitals increasingly rely on artificial intelligence–enabled clinical decision support systems, networked diagnostic tools, and data-intensive workflows that extend far beyond traditional perimeter-based security models. At the same time, healthcare delivery organizations remain structurally dependent on legacy medical devices and operating systems that were never designed for persistent connectivity or adversarial threat environments. This structural contradiction has produced a fragile cybersecurity landscape, repeatedly exposed through large-scale incidents and systemic vulnerabilities. Within this context, zero-trust architecture has emerged as a paradigmatic reconfiguration of cybersecurity governance, promising continuous verification, least-privilege access, and adaptive risk management across heterogeneous digital ecosystems. Yet the practical realization of zero trust in healthcare settings remains uneven, contested, and deeply constrained by socio-technical realities.

This article develops an original, theory-driven examination of zero-trust adoption in AI-enabled healthcare environments, with particular emphasis on clinical workstations and legacy medical devices. Drawing on an extensive, critical synthesis of interdisciplinary scholarship, policy reports, and technical analyses, the study interrogates how zero-trust principles intersect with artificial intelligence, blockchain-enabled security mechanisms, federated identity management, and explainable AI frameworks. Central to the analysis is the evaluation of operating system modernization strategies, including the adoption of Windows 11 in hospital clinical workstations, as a concrete site where zero-trust ideals confront institutional inertia, regulatory complexity, and embedded technological debt. The discussion integrates empirical insights from recent evaluative studies of hospital workstation environments, situating them within broader debates on accountability, trust, and risk in healthcare cybersecurity (Nayeem, 2026).

Methodologically, the article adopts a qualitative, interpretive research design grounded in systematic literature appraisal, comparative theoretical analysis, and socio-technical reasoning. Rather than privileging purely technical metrics, the study emphasizes governance structures, organizational learning processes, ethical accountability, and the co-evolution of human and machine agency in clinical contexts. The findings demonstrate that zero-trust implementation in healthcare is less a linear technological upgrade than a prolonged process of institutional transformation, requiring alignment between legacy infrastructures, regulatory regimes, and emerging AI-driven security practices. The article concludes by articulating a future research agenda that foregrounds adaptive governance, cross-sectoral standardization, and the moral economy of trust in digital medicine, arguing that cybersecurity resilience must be understood as a collective, dynamic achievement rather than a static technical endpoint.

Keywords: Zero-trust architecture; healthcare cybersecurity; legacy medical devices; artificial intelligence governance; clinical workstations; digital trust

INTRODUCTION

The contemporary healthcare sector occupies a paradoxical position within the global digital economy. On one hand, it stands at the forefront of technological innovation, embracing artificial intelligence–driven diagnostics, predictive analytics, telemedicine platforms, and data-intensive population health strategies.

On the other hand, it remains structurally constrained by deeply embedded legacy systems, regulatory fragmentation, and risk-averse organizational cultures that complicate the adoption of modern cybersecurity paradigms (Burrell, 2024). This paradox has become increasingly visible as healthcare organizations confront a sustained escalation in cyber incidents, ranging from ransomware attacks to data exfiltration and operational disruption, with direct implications for patient safety and public trust (Help Net Security, 2023).

Historically, healthcare cybersecurity evolved within a perimeter-based security logic, premised on the assumption that threats originated primarily outside organizational boundaries. Firewalls, network segmentation, and access control lists were designed to protect a relatively stable internal environment populated by trusted users and devices (Northcutt, 2005). While this model proved sufficient during earlier phases of health information technology adoption, it has been progressively undermined by the proliferation of mobile devices, cloud services, remote access requirements, and third-party integrations. The integration of artificial intelligence into clinical workflows further destabilizes perimeter assumptions by introducing opaque decision-making systems that rely on continuous data flows across organizational and sometimes national boundaries (Habli et al., 2020).

Zero-trust architecture has emerged as a response to these structural transformations, reframing cybersecurity not as a defensive boundary but as an ongoing process of verification, contextual risk assessment, and adaptive control (He et al., 2022). At its conceptual core, zero trust rejects implicit trust based on network location or device ownership, instead requiring continuous authentication, authorization, and monitoring of all entities interacting with digital resources. This paradigm shift has been widely promoted as particularly relevant to healthcare, where heterogeneous device ecosystems, sensitive data, and high-stakes operational requirements intersect (Gellert et al., 2023).

Despite its conceptual appeal, the translation of zero-trust principles into healthcare practice has proven deeply challenging. Hospitals operate complex assemblages of legacy medical devices, many of which rely on outdated operating systems, proprietary protocols, and vendor-controlled update cycles. Empirical assessments indicate that a substantial proportion of medical equipment in active clinical use continues to operate on unsupported or end-of-life operating systems, significantly constraining the feasibility of modern security controls (Kaspersky, 2024). These constraints are not merely technical but institutional, shaped by procurement practices, regulatory certification processes, and the ethical imperative to avoid disruptions to patient care.

Within this contested terrain, clinical workstations occupy a critical yet underexamined position. As the primary interface between clinicians and digital systems, workstations mediate access to electronic health records, AI-driven decision support tools, imaging platforms, and networked medical devices. Recent evaluative research has highlighted the strategic significance of workstation operating system modernization as a foundational step toward zero-trust implementation in hospital environments, particularly through the adoption of security-enhanced platforms such as Windows 11 (Nayeem, 2026). Such modernization efforts illuminate both the possibilities and limitations of aligning zero-trust ideals with legacy-dependent clinical infrastructures.

The existing literature on healthcare cybersecurity has tended to fragment along disciplinary lines, with technical studies focusing on architectural models, policy analyses emphasizing regulatory compliance, and ethical discussions addressing accountability and trust. While each perspective contributes valuable insights, their separation has limited the development of integrated frameworks capable of addressing the socio-technical complexity of zero-trust transformation in healthcare settings (Tyler & Viana, 2021). Moreover, much of the scholarship treats legacy systems as static obstacles rather than dynamic components of evolving organizational ecosystems.

This article seeks to address these gaps by advancing a comprehensive, theoretically grounded analysis of zero-trust adoption in AI-enabled healthcare, centered on the interaction between legacy medical devices, clinical workstations, and emerging cybersecurity governance models. By situating recent empirical evaluations of workstation modernization within broader debates on digital trust, institutional learning, and technological change, the study offers a nuanced account of how zero trust is negotiated, adapted, and sometimes resisted in practice (Nayeem, 2026). In doing so, it contributes to a more holistic understanding of cybersecurity resilience as a socio-technical achievement shaped by history, power, and ethical responsibility.

METHODOLOGY

The methodological approach underpinning this study is qualitative, interpretive, and integrative, reflecting the complex, multi-layered nature of cybersecurity transformation in healthcare environments. Rather than pursuing a narrowly empirical or purely technical evaluation, the research design emphasizes critical synthesis, theoretical elaboration, and contextual interpretation across diverse bodies of literature. This approach is particularly appropriate given the study's focus on zero-trust architecture, which operates not only as a technical framework but also as a governance philosophy embedded within organizational practices and regulatory regimes (Ghasemshirazi et al., 2023).

The primary methodological foundation of the study is an extensive critical review of peer-reviewed academic literature, complemented by authoritative policy reports, industry analyses, and evaluative case studies. Systematic principles derived from established review methodologies were applied to ensure rigor, transparency, and analytical coherence, drawing conceptually on frameworks such as PRISMA and mixed-methods appraisal tools without reducing the analysis to procedural checklists (Page et al., 2021; Hong et al., 2018). The emphasis throughout was on depth of interpretation rather than exhaustive enumeration of sources.

A central analytic strategy involved thematic synthesis, through which recurring concepts, tensions, and debates across the literature were identified and elaborated. Key thematic domains included zero-trust architecture principles, legacy system dependency, artificial intelligence governance, blockchain-enabled security mechanisms, and ethical accountability in healthcare technology. Within each domain, the analysis traced historical trajectories, theoretical foundations, and contemporary controversies, enabling a layered understanding of how these elements interact within real-world healthcare settings (Khan et al., 2025).

Particular methodological attention was devoted to integrating evaluative research on clinical workstations and operating system modernization. Recent studies examining the adoption of Windows 11 in hospital environments were treated not as isolated technical assessments but as empirical entry points into broader socio-technical dynamics (Nayeem, 2026). These studies were analyzed for their implicit assumptions, methodological limitations, and governance implications, situating their findings within the larger discourse on zero-trust feasibility in legacy-dependent infrastructures.

The study also employed comparative analytical reasoning, juxtaposing healthcare cybersecurity challenges with analogous developments in other critical infrastructure sectors. This comparative lens allowed for the identification of sector-specific constraints, such as patient safety imperatives and regulatory certification processes, that distinguish healthcare from more agile digital industries (Debnath, 2023). At the same time, it highlighted transferable lessons regarding organizational learning, identity management, and adaptive risk governance (Huda et al., 2024).

Methodological limitations are acknowledged as an integral component of scholarly rigor. The reliance on secondary sources necessarily constrains the ability to capture real-time organizational practices or informal decision-making processes. Moreover, the heterogeneity of healthcare systems across national and institutional contexts complicates the generalization of findings. Nevertheless, by foregrounding theoretical integration and critical interpretation, the study aims to generate conceptual insights with relevance across diverse healthcare environments, rather than prescriptive solutions tied to specific technical configurations.

RESULTS

The interpretive analysis of the literature reveals a complex and often contradictory landscape of zero-trust adoption in AI-enabled healthcare systems. One of the most salient findings is the pervasive gap between zero-trust principles as articulated in architectural models and their practical realization within hospital environments. While the theoretical literature consistently emphasizes continuous verification, least-privilege access, and micro-segmentation as foundational elements of zero trust, empirical accounts suggest that healthcare organizations struggle to operationalize these principles in the presence of legacy medical devices and entrenched workflows (He et al., 2022).

A recurring result across studies is the identification of clinical workstations as critical leverage points in zero-trust transformation. Workstations function as convergence nodes where user identity, device posture, application access, and data flows intersect. Evaluations of workstation modernization initiatives indicate

that upgrading operating systems can significantly enhance baseline security capabilities, including hardware-based isolation, secure boot processes, and improved identity integration (Nayeem, 2026). However, these technical gains are often offset by compatibility challenges with older medical applications and devices, reinforcing the persistent influence of technological debt.

The analysis further reveals that artificial intelligence plays an ambivalent role in healthcare cybersecurity. On one hand, AI-driven threat detection, behavioral analytics, and automated policy enforcement are widely promoted as essential enablers of zero-trust architectures (Ajish, 2024). On the other hand, concerns regarding explainability, accountability, and bias complicate the deployment of AI in safety-critical clinical contexts (Markus et al., 2021). The literature suggests that trust in AI-based security mechanisms is unevenly distributed among stakeholders, with clinicians often expressing skepticism toward opaque systems that influence access to critical resources (Habli et al., 2020).

Another significant result concerns the integration of blockchain technologies as complementary mechanisms for securing AI-driven healthcare systems. Systematic reviews highlight the potential of blockchain to enhance data integrity, auditability, and decentralized trust, particularly in environments characterized by multiple stakeholders and cross-organizational data sharing (Kasralikar et al., 2025). Nevertheless, the practical integration of blockchain within zero-trust frameworks remains largely experimental, constrained by scalability concerns, regulatory uncertainty, and the need for specialized expertise.

Across the reviewed literature, there is a consistent recognition that zero-trust adoption is not a one-time implementation but an ongoing process of organizational learning and governance adaptation. Studies emphasize the importance of aligning technical controls with institutional policies, workforce training, and ethical frameworks to sustain cybersecurity resilience over time (Tyler & Viana, 2021). This finding underscores the inadequacy of purely technical metrics for evaluating zero-trust success, pointing instead toward qualitative indicators such as risk awareness, cross-disciplinary collaboration, and adaptive capacity.

DISCUSSION

The findings of this study invite a deeper theoretical interrogation of zero-trust architecture as a socio-technical paradigm rather than a narrowly defined security model. At a conceptual level, zero trust represents a profound reconfiguration of how trust is produced, distributed, and governed within digital systems. In healthcare contexts, this reconfiguration intersects with longstanding ethical commitments to patient safety, professional autonomy, and institutional accountability, creating tensions that cannot be resolved through technical optimization alone (Gellert et al., 2023).

One of the central theoretical implications of the analysis is the need to reconceptualize legacy medical devices not merely as obstacles to modernization but as historically situated artifacts that embody past regulatory, economic, and clinical priorities. The persistence of outdated operating systems and proprietary protocols reflects decades of procurement practices oriented toward functional reliability rather than cybersecurity resilience. Zero-trust initiatives that fail to engage with this historical layering risk reproducing superficial compliance rather than substantive transformation (Vijayasekhar, 2022).

The evaluation of Windows 11 adoption in clinical workstations provides a concrete illustration of these dynamics. While enhanced security features align closely with zero-trust principles, their effectiveness depends on organizational willingness to re-engineer workflows, renegotiate vendor relationships, and invest in workforce training (Nayeem, 2026). This underscores the argument that zero trust is best understood as an institutional project, requiring sustained governance commitment rather than isolated technical upgrades.

Artificial intelligence further complicates this landscape by introducing new forms of epistemic authority into cybersecurity decision-making. AI-driven systems promise efficiency and scale but also challenge traditional notions of accountability, particularly when security decisions affect clinical access and patient outcomes. The literature's emphasis on explainable AI highlights the ethical imperative to render algorithmic processes intelligible to human stakeholders, thereby sustaining trust within complex socio-technical systems (Markus et al., 2021).

From a governance perspective, the discussion reveals a growing consensus that healthcare cybersecurity must be addressed through adaptive, multi-level frameworks that integrate technical controls, regulatory oversight, and ethical deliberation. Zero-trust architecture offers a compelling organizing principle for such

frameworks, but its realization depends on the alignment of incentives, norms, and institutional capacities across diverse actors (Burrell, 2024). Future research must therefore move beyond architectural blueprints to examine the lived experiences of zero-trust transformation within healthcare organizations.

CONCLUSION

This article has advanced a comprehensive, theory-driven analysis of zero-trust architecture in AI-enabled healthcare environments, foregrounding the socio-technical challenges posed by legacy medical devices and clinical workstation infrastructures. By critically synthesizing interdisciplinary scholarship and integrating empirical insights from recent evaluative studies, the analysis demonstrates that zero-trust adoption is a complex, contested process shaped by historical dependencies, ethical imperatives, and organizational governance dynamics (Nayeem, 2026).

The study concludes that cybersecurity resilience in healthcare cannot be achieved through technical solutions alone. Instead, it requires a sustained commitment to institutional learning, cross-sector collaboration, and ethical accountability. Zero-trust architecture provides a valuable conceptual framework for navigating this transformation, but its success ultimately depends on the capacity of healthcare organizations to reconcile innovation with the enduring realities of legacy systems and patient-centered care.

REFERENCES

1. Kasralikar, P., Polu, O. R., Chamarthi, B., Rupavath, R. V. S. S. B., Patel, S., & Tumati, R. (2025). Blockchain for securing AI-driven healthcare systems: A systematic review and future research perspectives. Cureus, 17, e83136.
2. Northcutt, S. (2005). Inside network perimeter security (2nd ed.). Sams.
3. Help Net Security. (2023). Rising cyber incidents challenge healthcare organizations.
4. Nayeem, M. (2026). 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, 3(1), 1–8. https://doi.org/10.64917/feaiml/Volume03Issue01-01
5. Gellert, G. A., et al. (2023). Zero trust and the future of cybersecurity in healthcare delivery organizations. Journal of Hospital Administration, 12(1), 1–8.
6. Habli, I., Lawton, T., & Porter, Z. (2020). Artificial intelligence in health care: Accountability and safety. Bulletin of the World Health Organization, 98, 251–256.
7. Burrell, D. N. (2024). Understanding healthcare cybersecurity risk management complexity. Land Forces Academy Review, 29, 38–49.
8. He, Y., et al. (2022). A survey on zero trust architecture: Challenges and future trends. Wireless Communications and Mobile Computing, 1–13.
9. Debnath, S. (2023). Integrating information technology in healthcare: Recent developments, challenges, and future prospects for urban and regional health. World Journal of Advanced Research and Reviews, 19(1), 455–463.
10. Markus, A. F., Kors, J. A., & Rijnbeek, P. R. (2021). The role of explainability in creating trustworthy artificial intelligence for health care: A comprehensive survey. Journal of Biomedical Informatics, 113, 103655.
11. Ajish, D. (2024). The significance of artificial intelligence in zero trust technologies: A comprehensive review. Journal of Electrical Systems and Information Technology, 11, 30.
12. Tyler, D., & Viana, T. (2021). Trust no one? A framework for assisting healthcare organisations in transitioning to a zero-trust network architecture. Applied Sciences, 11(16), 1–18.
13. Vijayasekhar, D. (2022). Securing the future: Strategies for modernizing legacy systems and enhancing cybersecurity. Journal of Artificial Intelligence and Cloud Computing, 1(3), 1–3.
14. Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023). Zero trust: Applications, challenges, and opportunities. arXiv, 1–23.
15. Kaspersky. (2024). Kaspersky finds 73% of healthcare providers use medical equipment with a legacy OS.
16. Page, M. J., McKenzie, J. E., Bossuyt, P. M., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71.

17. Hong, Q. N., Pluye, P., Fàbregues, S., et al. (2018). Mixed methods appraisal tool (MMAT), version 2018. BMJ, 1–7.
18. Khan, M. M., Shah, N., Shaikh, N., Thabet, A., Alrabayah, T., & Belkhair, S. (2025). Towards secure and trusted AI in healthcare: A systematic review of emerging innovations and ethical challenges. International Journal of Medical Informatics, 195, 105780.
19. Kaul, D. (2019). Blockchain-powered cyber-resilient microservices: AI-driven intrusion prevention with zero-trust policy enforcement. Journal of Mathematical and Computational Science, 1–34.
20. Huda, S., Islam, M. R., Abawajy, J., Kottala, V. N., & Ahmad, S. (2024). A cyber risk assessment approach to federated identity management framework-based digital healthcare system. Sensors, 24, 5282.
21. Ofili, B. T., Erhabor, E. O., & Obasuyi, O. T. (2025). Enhancing federal cloud security with AI: Zero trust, threat intelligence, and compliance. World Journal of Research and Review, 25, 2377–2400.
22. Shojaei, P., Vlahu-Gjorgievska, E., & Chow, Y. W. (2024). Security and privacy of technologies in health information systems: A systematic literature review. Computers, 13(2), 1–25.
23. Mandiant. (2022). M-Trends 2022 special report: Executive summary.
24. Ho, G., et al. (2021). Hopper: Modeling and detecting lateral movement (extended report). arXiv, 1–20.
25. Department of Health. (2018). Investigation: WannaCry cyber-attack on the NHS. UK National Audit Office.
26. Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. World Journal of Advanced Research and Reviews, 19(3), 105–116.
27. Eastwood, B. (2024). Tips for health systems on managing legacy systems to strengthen security. HealthTech Magazine.
28. International Conference on Communication Technologies (ComTech 2017). (2017). Institute of Electrical and Electronics Engineers.