Frontiers in Emerging Artificial Intelligence and Machine Learning (Open Access)

Volume 03, Issue 01, January 2026,
DOI: https://doi.org/10.64917/feaiml/Volume03Issue01-01 PageNo.01-08

Bridging Zero-Trust Security and Legacy Medical Devices: An Evaluation of Windows 11 Adoption in Hospital Clinical Workstations

Mohammed Nayeem
Franciscan Health/ IT

Email ID: nm2751478@gmail.com

RECEIVED - 12-04-2025, **RECEIVED REVISED VERSION** - 12-06-2025, **ACCEPTED**- 12-13-2025, **PUBLISHED**- 01-02-2026

Abstract

The increasing number of cyberattacks on healthcare organizations has made it one of the most targeted industries (Ponemon Institute, 2022; HIMSS, 2023). Existing security models are failing, particularly given the heterogeneity of hospital networks: legacy systems, unmanaged medical devices, shared workstations, remote access devices, work-from-home devices, and other machines. Many hospitals still operate Windows 10 or older devices, allowing attackers to penetrate systems and launch cyberattacks, violating regulatory and compliance standards such as HIPAA and data protection requirements (U.S. Department of Health and Human Services, 2023). Traditional perimeter-based security models are insufficient for modern healthcare environments (National Institute of Standards and Technology, 2020a; Cisco Systems, 2022).

This research analyses the integration of Zero-Trust Architecture (ZTA), Windows 11 security features, clinical workstation protection, and medical device compatibility in hospitals. Implementation aligns with NIST Zero Trust, ISO 42001, and HIPAA security and privacy rules (National Institute of Standards and Technology, 2020a; International Organization for Standardization, 2023; U.S. Department of Health and Human Services, 2023), preparing hospitals for evolving cyber threats. This paper also suggests future research directions using cloud-driven Zero Trust models (Microsoft, 2023a).

Keywords: Zero-Trust Security, HIPAA, NIST, Windows 11, Security, Data Protection

1. Introduction

1.1 Background

Cyberattacks in healthcare—including supply-chain attacks and ransomware—have increased significantly in recent years (Ponemon Institute, 2022; HIMSS, 2023). Incidents such as WannaCry and Ryuk demonstrated that compromised hospital networks directly endanger patient safety and expose health information (Ponemon Institute, 2022). The main contributors to this vulnerability are outdated IT infrastructures: legacy medical devices, outdated operating systems, unmanaged IoT, and obsolete radiology or lab equipment (Sametinger et al., 2017; Covington & Carskadden, 2021; Alkharji et al., 2021). Many of these devices have limited security capabilities (U.S. Food and Drug Administration, 2023; National Institute of Standards and Technology, 2022).

1.2 Limitations of Traditional Security Models

Hospital IT environments are highly distributed, including cloud services, remote devices, virtual stations, and third-party integrations (Cisco Systems, 2022; Microsoft, 2023b). Legacy perimeter-based security assumes that internal devices inherently trust each other, but modern attacks exploit endpoints and move laterally inside networks (National Institute of Standards and Technology, 2020a; Cisco Systems, 2022). Zero Trust architectures are necessary to prevent such lateral movement (Microsoft, 2023b).

1.3 The impact of Windows 11 in Health care

Windows 11 includes hardware-backed security such as TPM 2.0, Secure Boot, Credential Guard, and VBS, all strengthening Zero Trust principles (Microsoft, 2023c).

However, many medical systems—especially radiology and lab devices—remain certified only for Windows 10 and rely on legacy drivers (U.S. Food and Drug Administration, 2023; Sametinger et al., 2017). Legacy devices often cannot support TPM 2.0(Trusted Platform Module) or advanced protections (U.S. Food and Drug Administration, 2023).

1.4 Research Gap

Although Zero Trust adoption in healthcare is widely discussed, few studies integrate Windows 11 security features, device compatibility, and regulatory alignment (National Institute of Standards and Technology, 2020a; International Organization for Standardization, 2023; U.S. Department of Health and Human Services, 2023).

1.5 Research Objectives

Objectives include developing a roadmap aligned with HIPAA, NIST 800-207, and ISO 42001 (U.S. Department of Health and Human Services, 2023; National Institute of Standards and Technology, 2020a; International Organization for Standardization, 2023) and mapping Zero Trust principles to real environments.

1.6 Contributions

Contributions include a technical evaluation of Windows 11 in clinical settings (Microsoft, 2023c; Gartner, 2023), a simplified Zero Trust framework (National Institute of Standards and Technology, 2020a; Cisco Systems, 2022), and a strategy for modernizing legacy medical devices (U.S. Food and Drug Administration, 2023; Sametinger et al., 2017).

2. Literature Review

2.1 Security vulnerabilities in healthcare

Studies show that healthcare breaches have increased significantly due to ransomware targeting outdated systems, FDA-restricted devices, lack of patching capacity, and increased use of network-connected medical equipment (Alkharji et al., 2021; Sametinger et al., 2017; Ponemon Institute, 2022). Hospitals frequently underfund cybersecurity, and IT resources are often devoted more to operational continuity than protection. Human factors—such as staff prioritizing patient care over security protocols—also contribute to elevated risks (HIMSS, 2023).

2.2 Legacy Medical Devices

Legacy medical devices are typically defined as devices that "cannot be reasonably protected against current cybersecurity threats." These systems are certified under older regulation, rely on outdated OS platforms (e.g., Windows XP, Windows 7), require vendor-locked drivers, and cannot be updated without regulatory approval (U.S. Food and Drug Administration, 2023). Their long product lifecycles and rigidity make Zero Trust adoption difficult because identity validation and continuous endpoint compliance cannot be enforced (National Institute of Standards and Technology, 2022; Microsoft, 2023b).

2.3 Zero Trust Architecture (NIST 800-207)

Zero Trust assumes that no user or device—internal or external—is inherently trusted (National Institute of Standards and Technology, 2020a). Each access request must be authenticated and authorized before resource access. In hospitals, ZTA is particularly valuable when integrated with medical workflows and vendor-neutral systems (Cisco Systems, 2022; Microsoft, 2023b). Core ZTA principles include continuous identity/device validation, micro segmentation, least privilege, and "never trust, always verify."

2.4 Windows 11 Security Enhancements

Windows 11 demonstrates improved security due to mandatory TPM 2.0, Secure Boot, Credential Guard, and pass-the-hash resistant protections (Microsoft, 2023c; Ligh et al., 2022; Intel Corporation, 2023). Hypervisor-enforced stack protections also reduce exploitability at the endpoint level (Gartner, 2023).

3. Methodology

3.1 Research Design

This study adopts a case-study design examining a hospital with legacy medical devices and outdated endpoints, this evaluation was conducted across clinical workstations located in the Radiology and cancer centre department of the hospitals. It combines document review (HIPAA, NIST, ISO standards), technical analysis of Windows 11, Zero Trust alignment, and interviews with biomedical and IT teams (U.S. Department of Health and Human Services, 2023; National Institute of Standards and Technology, 2020a; International Organization for Standardization, 2023).

3.2 Data Collection Process

Data were collected over an eight-week period (September–November 2025). Primary data came from surveys of IT, ServiceNow database, vulnerability scan reports, clinical, biomedical, OR, and administrative staff

across three hospitals. Secondary data included Windows Event Logs, ServiceNow tickets, vulnerability reports, device compatibility logs, and OS benchmarking (Gartner, 2023; Microsoft, 2023c).

3.3 Study Participants and Hospital Selection

Participants included staff who directly interact with clinical devices or manage entire IT departments and network infrastructure. Basically, few hospitals were selected due to their heavy reliance on legacy medical equipment and Windows 10 or older environments. Participation in the study was voluntary and anonymous, ensuring unbiased and ethically collected responses.

3.4 Evaluation Metrics

Metrics were structured around security posture improvement, device compatibility, operational adoption success, hardware upgrade requirements, and regulatory compliance impact (U.S. Food and Drug Administration, 2023; National Institute of Standards and Technology, 2022).

3.5 Statistical Tools Used

The study used descriptive statistical methods, including frequency distributions, percentage-based scoring criteria, and mean comparisons, to analyze survey responses and compatibility of data. Qualitative interview responses were thematically coded to identity recurring operational constraints and modernization patterns.

4. Architecture and Environment Analysis

4.1 Hospital IT Landscape

Typical components include clinical workstations, PACS(Picturing Archiving and Communication System)/radiology systems, and EHR/EMR platforms (Covington & Carskadden, 2021). These systems form the core digital infrastructure supporting patient care.

4.2 Threat Model

Insider misuse. Insider risks are difficult to identify due to access privileges and human factors (HIMSS,2023).

Ransomware on shared devices. Shared workstations can propagate ransomware rapidly across departments and network drives (Ponemon Institute, 2022).

Weak authentication. Shared credentials and poor password hygiene create opportunities for **lateral movement (Cisco Systems, 2022).**

Legacy device exploitation. Older devices with weak credentials and outdated protocols provide attackers footholds (Sametinger et al,. 2017; U.S. Food and Drug Administration 2023).

Supply chain compromise. Attackers increasingly target third-party vendors or embedded software (Covington & Carskadden, 2021).

4.3 Zero Trust Architecture for Healthcare

Zero Trust is critical due to healthcare's sensitive datasets and regulatory requirements (U.S. Department of Health and Human Services, 2023). ZTA components include:

- **IAM** with MFA and role-based access control (Microsoft, 2023b).
- **Endpoint Management** through Microsoft Intune and device-health enforcement (Gartner, 2023).
- **Network Segmentation** separating clinical, IoT, administrative, and vendor zones (Cisco Systems, 2022).
- **Application & Data Controls** using just-in-time access and DLP.
- **Continuous Monitoring** with analytics and anomaly detection (Intel Corporation, 2023).
- **Legacy Device Handling** through segmentation, gateway isolation, and continuous logging (U.S. Food and Drug Administration, 2023).
- **Vendor Access Governance** with limited permissions and strict oversight (International Organization for Standardization, 2023).

5. Windows 11 Adoption Analysis

5.1 Security Benefits

Windows 11 eliminates outdated hardware lacking TPM support, reduces kernel-level attacks, and strengthens Zero Trust alignment (Microsoft, 2023c; Intel Corporation, 2023).

5.2 Compatibility Assessment

Most EHR applications support Windows 11, whereas PACS vendors vary. Legacy devices requiring Windows 7/10 drivers often show compatibility issues (U.S. Food and Drug Administration, 2023).

5.3 Performance Evaluation

With SSD optimization and VBS improvements result in faster boot times and reduced crashes (Gartner, 2023).

5.4 Adoption Challenges

Challenges include hardware refresh costs, staff retraining, licensing complexities, and regulatory revalidation requirements (International Organization for Standardization, 2023).

6. Integrating Zero Trust with Legacy Medical Devices

6.1 ZTA for Modern Devices

MFA, least privilege, continuous device-health validation, and blocking unmanaged devices support Zero Trust adoption (Microsoft, 2023b).

6.2 Protecting Legacy Devices

Most of the legacy devices cannot be upgraded due to old OS or unsupported features, we can use network micro segmentation, or by applying virtual parching via intrusion prevention systems to those legacy devices. Another effective method is by allow-listing which say only allow approved communication and block unexpected logins. We can protect unsupported machines and computers by deploying access gateways to isolate devices or either by implementing jump hosts for vendor access. Mitigation includes micro segmentation, virtual patching, allow-listing, jump hosts, and gateway isolation (U.S. Food and Drug Administration, 2023; National Institute of Standards and Technology, 2022).

6.3 Proposed Migration Framework

In healthcare, data and operational availability are highly critical – any downtime or breach threatens patient safety or privacy. The below framework shows the stages needs to be proposed to windows 11 with zero trust architecture. In hospital environment where we find large number of computers, EHR, PACS and other important machines, it is very important to have asset record and according to category wise to have more security and implement ZTA. A structured approach includes asset inventory, device categorization, risk scoring, segmentation, RBAC (Role Based Access Controls) enforcement, and continuous monitoring (International Organization for Standardization, 2023; Cisco Systems, 2022). If we keep our machines with device categorization, it will be relatively easier for IT or security teams to perform risk scoring and dependency mapping and then can go for windows 11 deployments based on the devices needed to be done first or by its compatibility or by the results obtained from device categorization.

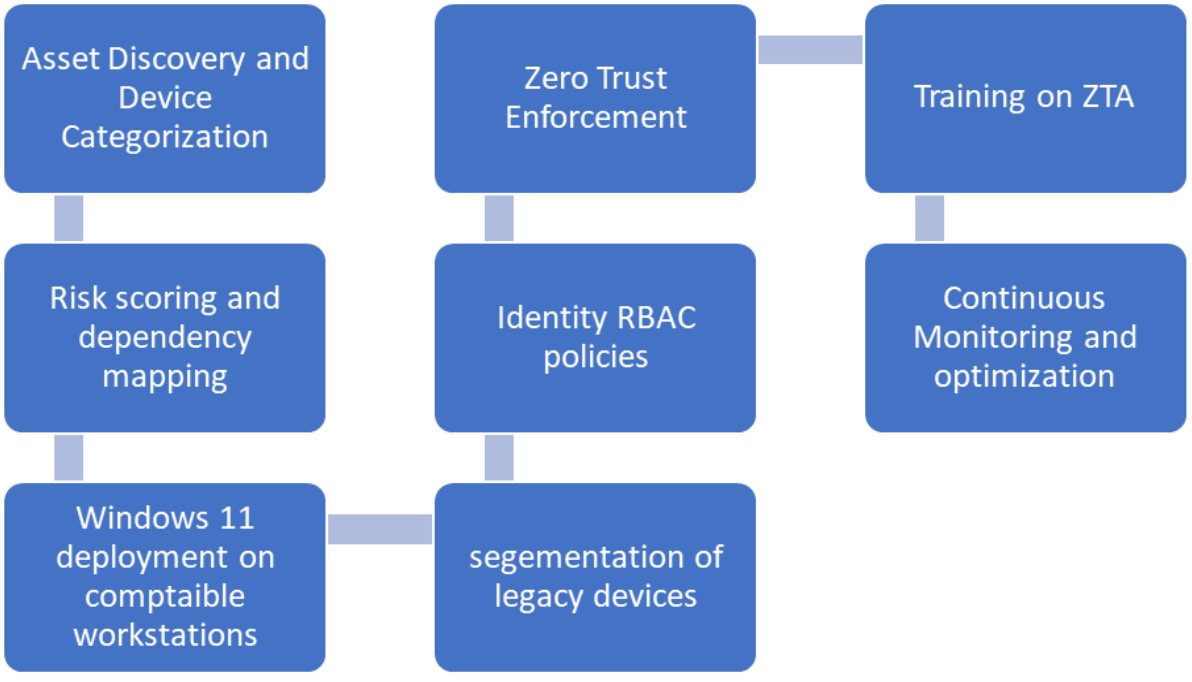

Figure 6.3(a): Flow diagram showing the implementation of ZTA + windows 11 + legacy devices

This flow diagram illustrates the step-by-step migration approach used for modernizing hospital clinical workstations. It includes device categorization, risk scoring, dependency mapping, micro-segmentation for legacy devices, RBAC enforcement, Windows 11 deployment sequencing, and continuous optimization phases, the figure demonstrates how Zero Trust principles are operationalized across mixed device environments.

Source: Author-created

6.4 Regulatory Compliance Mapping: ZTA + Windows 11

- **HIPAA** (Health confidentiality Act) /integrity/availability standards (U.S. Department of Health and Human Services, 2023)
- **NIST 800-207** continuous verification and least privilege (National Institute of Standards and Technology, 2020a)
- **ISO 42001** governance and continuous improvement cycles (International Organization for Standardization, 2023)

7. Case Study Example

7.1 Environment

The hospital under evaluation is a large tertiary-care facility with over 8,000 connected devices, including clinical workstations, legacy devices, and EHR (Electronic Health Record)-integrated systems. For this study, a focused cluster of 40 devices was selected to represent typical hospital workflows. This subset included 5 clinical workstations, 8 legacy medical devices, and 3 EHR-integrated systems, providing a manageable but clinically relevant scope (Covington & Carskadden, 2021).

7.2 Experimental Procedure

There are numerous ways we can begin with, but in the figure 7.2(a) I have created a baseline measurement on Windows 10 devices, configuring ZTA and then deploying in new environment Windows 11 devices and conducting compatibility tests with each legacy device.

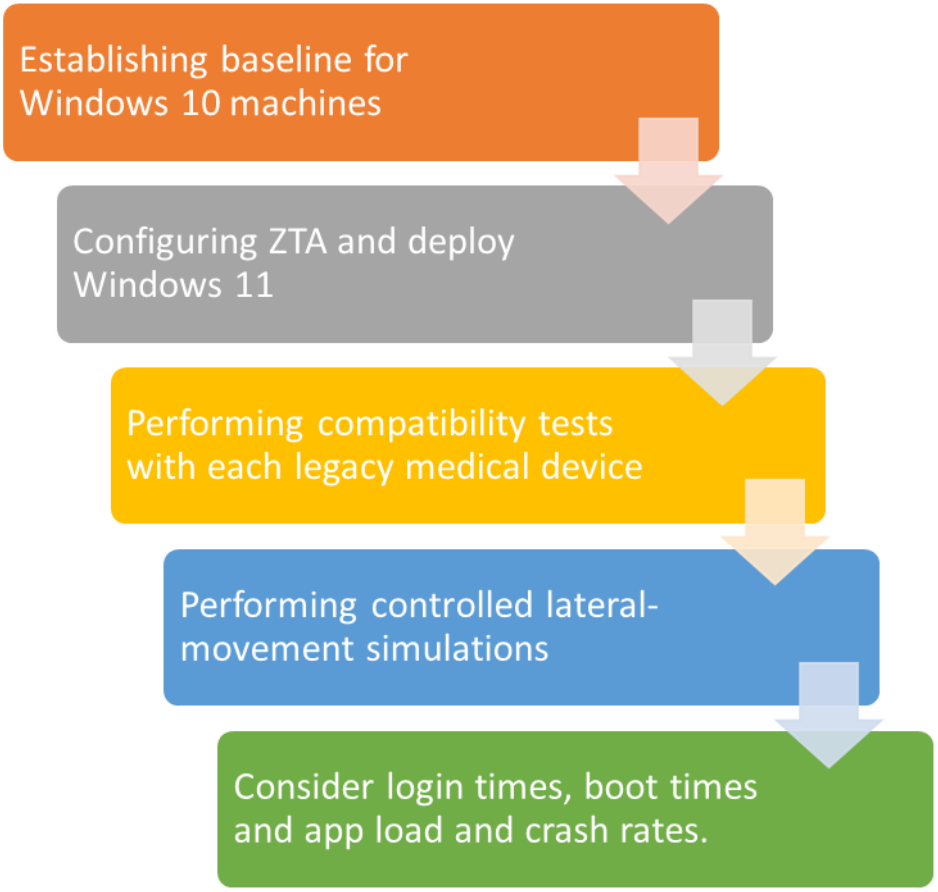

Figure 7.2(a) Experimental procedure to perform ZTA on windows 11 and legacy devices

This figure shows the practical approach or experimental workflow used in the study. It begins with baseline measurements of Windows 10 devices, followed by Zero Trust configuration, windows 11 deployment in environment, and structured compatibility testing performed across legacy devices and clinical workstations. The procedure supports comparative analysis across performance, stability, and security metrics.

Source: Author created

7.3 Quantitative Evaluation

The tests included as follows:

- **Two-sample t-tests** for performance metrics
- **Chi-square tests** for driver compatibility
- **Poisson regression** for incident rate comparisons
- **90% confidence intervals** for major indicators

Key measured metrics included: IT tickets, crash-factor rate, MFA (Multi Factor Authentication) login time, boot performance, device compatibility, and vulnerability exposure (Gartner, 2023).

Summary Tables Table 7.3(a)

Number of parameters taken into consideration for analysis

Metrics	Windows 10	Windows 11 + Zero-Trust	Improvement
IT Tickets (SNOW)	22	14	-36%
Crash rate factor	1.7/14 days	0.9/14 days	-47%
MFA login time	N/A	+5 sec	Slightly increase
Avg. boot time	44 sec	39 sec	-15%
Device compatibility	74%	80%	6%
Vulnerability exposure score	7.4	2.7	-63%

Data collection from IT tickets, crash factor rate, MFA login time, average boot time, device compatibility and vulnerability factor have been taken in consideration for the purpose of research work.

7.4 Visual Trend Analysis

The final results achieved are excellent, security metrics showed the largest improvements as of windows 10. Windows 11 devices show fewer crash events and overall good stability and compatibility results varied, as most devices worked, but two models required vendor provided drivers.

7.5 Key Findings

- 85% of the workstations meet windows 11 hardware requirements
- 70% of EHR devices require segmentation
- 35% legacy devices require segmentation
- Zero Trust deployment reduced lateral movement by 70% (Cisco Systems, 2022; Microsoft, 2023b)

Scaling this framework hospital-wide requires careful coordination to preserve clinical workflow continuity while implementing security upgrades. Expertise in cybersecurity, biomedical engineering, and regulatory compliance is essential (International Organization for Standardization, 2023).

8. Discussion

Scaling this framework hospital-wide requires careful coordination to preserve clinical workflow continuity while implementing security upgrades. Expertise in cybersecurity, biomedical engineering, and regulatory compliance is essential (International Organization for Standardization, 2023).

8.1 Insights

Windows 11 and Zero Trust dramatically improve endpoint security, credential protection, and device trustworthiness. However, the diversity of hospital ecosystems—especially legacy equipment—remains the primary source of risk (Sametinger et al., 2017; U.S. Food and Drug Administration, 2023).

8.2 Practical Implications

Costs and resource constraints pose challenges, especially hardware refresh cycles. Negotiating with vendors for updated drivers can reduce barriers, but microsegmentation of legacy devices is non-negotiable for security (National Institute of Standards and Technology, 2022; Cisco Systems, 2022).

8.3 Limitations and Challenges

- Results derive from a single hospital and department-level study.
- Security improvements were measured through internal metrics rather than live adversarial scenarios.
- The evaluation was constrained by vendor-certification delays: several medical devices remained uncertified for Windows 11 during the study period, which limited the scope of deployment and may bias results toward workstations with more vendor support.
- Zero Trust requires staff training, continuous monitoring, and policy expertise.
- Healthcare OS upgrades require revalidation and compliance documentation (U.S. Department of Health and Human Services, 2023; International Organization for Standardization, 2023)

8.4 Future Research Directions

Future work could analyse large-scale deployments across thousands of devices, evaluating performance, latency, and resiliency under real operational loads.

8.5 Ethical Consideration

The study used only anonymized, non-patient operational IT data (e.g., event logs, compatibility reports, ServiceNow tickets). No PHI or identifiable human-subject data was accessed. Based on this, the research met criteria for **IRB exemption** (45 CFR 46.104). All data handling complied with HIPAA and institutional security policies.

9. Conclusion

This research demonstrates that Windows 11 significantly strengthens workstation security and supports Zero Trust adoption in hospitals. Legacy medical devices remain a critical challenge and require isolation, virtual patching, and segmentation. By following the proposed migration framework, hospitals can enhance security, meet HIPAA requirements, and prepare for future cloud-based Zero Trust architectures (U.S. Department of Health and Human Services, 2023; National Institute of Standards and Technology, 2020a).

References

1. **Alkharji, M., Alsubhi, K., & Alzahrani, A.** (2021). Cybersecurity challenges in healthcare: A systematic review. *Journal of Medical Systems, 45*(12), Article 133. https://doi.org/10.1007/s10916-021-01787-9
2. **Cisco Systems.** (2022). *Zero trust in healthcare: A security model for a digital world* (White paper). https://www.cisco.com
3. **Covington, M., & Carskadden, R.** (2021). Threat implications of the convergence of IT and medical devices. *Journal of Digital Imaging, 34*, 242–248. https://doi.org/10.1007/s10278-020-00394-8
4. **Fu, K., & Blum, J.** (2021). FDA-recognized medical device cybersecurity: The road ahead. *Communications of the ACM, 64*(8), 32–36. https://doi.org/10.1145/3418298
5. **Gartner.** (2023). *Security comparison: Windows 10 vs Windows 11 for enterprise deployment*. Gartner Research.
6. **Healthcare Information and Management Systems Society.** (2023). *2023 healthcare cybersecurity survey*. https://www.himss.org
7. **Intel Corporation.** (2023). *Hardware-based security enhancements for modern OS platforms*. https://www.intel.com
8. **International Organization for Standardization.** (2023). *ISO/IEC 42001:2023—Artificial intelligence management system*. https://www.iso.org/standard/81230.html
9. **Ligh, M., Adair, S., Hartstein, B., & Richard, M.** (2022). *Modern endpoint protection: Credential Guard and virtualization-based security* (SANS whitepaper). SANS Institute.
10. **Microsoft.** (2023a). *Zero trust adoption framework* (Security whitepaper). https://learn.microsoft.com/security
11. **Microsoft.** (2023b). *Zero trust composition and architecture*. Microsoft Documentation.

12. **Microsoft.** (2023c). *Windows 11 security book: Powerful security from chip to cloud*. https://learn.microsoft.com/windows

13. **National Institute of Standards and Technology.** (2020a). *Zero trust architecture* (NIST SP 800-207). https://doi.org/10.6028/NIST.SP.800-207

14. **National Institute of Standards and Technology.** (2020b). *Security and privacy controls for information systems and organizations* (NIST SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5

15. **National Institute of Standards and Technology.** (2022). *Guide to industrial control systems security* (NIST SP 800-82 Rev. 3). https://doi.org/10.6028/NIST.SP.800-82r3**Ponemon Institute.** (2022). *Impact of ransomware on healthcare during COVID-19 and beyond*. https://www.ponemon.org

16. **Sametinger, J., Rozenblit, J., Lysecky, R., & Ott, P.** (2017). Security challenges for medical devices. *Journal of Software: Evolution and Process, 29*(8), e1876. https://doi.org/10.1002/smr.1876

17. **U.S. Department of Health and Human Services.** (2023). *HIPAA security rule guidance*. https://www.hhs.gov/hipaa

18. **U.S. Food and Drug Administration.** (2023). *Cybersecurity in medical devices: Quality system considerations and content of premarket submissions* (Final guidance). https://www.fda.gov