Computer Fraud and Security
ISSN (online): 1873-7056

Healthcare Zero-Trust Resilience Architecture (HZTRA): A Practitioner-Led Reference Model for Securing Hospital Information Systems

Susil Kumar Sahu

solution engineer executive advisor, elevance health, 740w peachtere St Nw Attanta , GA 30308 (USA)

email- susil.sahu@elevancehealth.com

This article presents work led by a healthcare information technology architect who has designed and implemented large-scale hospital information systems and cybersecurity controls across multi-hospital networks. The Healthcare Zero-Trust Resilience Architecture (HZTRA) described below formalises architectural patterns that have been applied in practice to protect mission-critical clinical environments and are intended to be reusable by hospitals and vendors internationally.

Abstract

Background: Hospitals are rapidly adopting electronic health records, connected medical devices, and telehealth platforms, which has expanded their digital attack surface and exposed them to frequent cyber incidents such as ransomware and data breaches. Traditional perimeter-based security architectures are increasingly inadequate for protecting complex, highly connected clinical environments. Objective: This article introduces the Healthcare Zero-Trust Resilience Architecture (HZTRA), a practitioner-developed zero-trust cybersecurity reference architecture tailored to hospital information systems and connected medical devices. The goal is to capture, in a reusable form, design patterns that have already been applied in large hospital networks to improve resilience against cyberattacks while preserving clinical workflows. Methods: A narrative review of the healthcare cybersecurity literature was combined with lessons learned from leading the design and rollout of hospital information systems and security controls in multi-hospital environments. Insights from published research on cyberthreats, medical device vulnerabilities, and zero-trust frameworks were synthesised with implementation experience to derive a pragmatic reference architecture that reflects typical hospital technology stacks, network topologies, and operational constraints. Results: The HZTRA organises hospital cybersecurity into five integrated domains: identity and access management, network micro-segmentation, medical device and Internet of Medical Things protection, application-level controls for critical clinical systems, and continuous monitoring with incident response. Each domain is mapped to common hospital components such as electronic health records, diagnostic systems, and bedside devices, demonstrating how zero-trust policies can be applied end-to-end in real deployments. Conclusions: Adopting the HZTRA can help hospitals reduce lateral movement opportunities for attackers, limit the impact of successful breaches, and enhance overall cyber resilience. Because the model distils patterns proven in large-scale projects, it provides chief information officers, security architects, and clinical leaders with a credible, experience-based blueprint for planning phased adoption of zero-trust in hospital environments and a concrete reference point for evaluating cybersecurity strategies.

1. Introduction

1.1 Cybersecurity challenges in modern hospitals

Over the past decade, hospitals have undergone rapid digital transformation, driven by the widespread adoption of electronic health records, connected diagnostic platforms, and telehealth services. This digitalisation has increased dependence on information technology for core clinical workflows and critical care. At the same time, healthcare organisations have become prime targets for ransomware, data exfiltration, and other cyberattacks, with incidents frequently disrupting services and compromising patient data. Industry and academic reports increasingly characterise healthcare as one of the most targeted sectors for cybercrime.

1.2 Limitations of perimeter-based security

Many hospitals still rely on perimeter-centric security models that assume a trusted internal network and untrusted external networks. In environments that include legacy systems, vendor-managed medical devices, and multiple third-party integrations, these assumptions no longer hold. Once an attacker gains a foothold, flat or weakly segmented networks allow lateral movement to high-value clinical systems such as electronic health records and imaging platforms, increasing the

potential impact of each breach. Several high-profile incidents have demonstrated that traditional approaches can fail even in organisations with significant security investments.

1.3 Zero-trust as an emerging paradigm for healthcare

Zero-trust security architectures challenge the notion of a trusted internal network by enforcing the principles of 'never trust, always verify' and least-privilege access. Access to applications and data is granted based on strong identity verification, continuous assessment of device posture, and strict micro-segmentation, rather than simple network location. While zero-trust has gained momentum in the broader enterprise security community, hospitals often lack detailed guidance on how to adopt these principles without disrupting time-critical clinical workflows or compromising patient safety.

1.4 Gaps in existing healthcare cybersecurity architectures

Existing frameworks for healthcare cybersecurity often focus on high-level policies, technical controls in isolation, or generic network architectures that do not fully reflect the complexity of hospital environments. Prior work has highlighted persistent vulnerabilities related to legacy systems, heterogeneous medical devices, human factors, and organisational constraints, and has called for more integrated, sociotechnical solutions. However, there remains a shortage of healthcare-specific zero-trust reference architectures that are grounded in real implementation projects and can be used as templates by other organisations.

1.5 Aim and contributions of this article

This article addresses this gap by presenting the Healthcare Zero-Trust Resilience Architecture (HZTRA), a zero-trust cybersecurity reference architecture specifically designed for hospital information systems and connected medical devices. The contributions are three-fold: (1) to summarise key themes from the healthcare cybersecurity literature that impact architectural design in hospitals; (2) to define a practical, layered zero-trust reference architecture that aligns with common hospital technology stacks and clinical workflows; and (3) to capture and formalise design patterns from large-scale implementation projects so that other institutions can adopt and adapt them, thereby extending the impact of the work beyond the author’s direct engagements.

2. Novelty and Significance of the HZTRA

The HZTRA is intended to be more than a restatement of generic zero-trust principles. It integrates requirements that are specific to hospitals, such as the need to maintain uninterrupted access to clinical systems, support vendor-managed medical devices, and comply with stringent privacy and safety regulations. By explicitly combining identity, segmentation, device protection, application security, and monitoring into a single, healthcare-focused model, the architecture fills a gap left by technology-agnostic enterprise frameworks.

A distinctive feature of the HZTRA is that it is derived from hands-on architectural leadership in complex hospital environments rather than designed purely in an academic setting. The patterns it describes have already been applied during the rollout and hardening of electronic health record platforms and associated systems in large, multi-site hospital networks. As a result, the architecture reflects not only what is theoretically desirable but also what has been shown to be feasible and sustainable in production, giving it practical significance for the wider healthcare community.

Because the HZTRA is expressed as a reusable reference model, it can be adopted, extended, and critiqued by other architects, vendors, and researchers. Over time, citations, adaptations, and external implementations can provide independent evidence of the model’s influence on the field. This potential for uptake and reuse is central to its value as an original contribution of significance to healthcare cybersecurity practice.

3. Background and Methods

The development of the HZTRA was informed by two complementary inputs. The first was a narrative review of peer-reviewed literature, standards, and authoritative reports on healthcare cybersecurity, medical device security, and zero-trust architectures. This review helped identify common threat patterns, recommended controls, and pre-existing architectural models relevant to hospitals. The second input was the author’s direct experience leading the design and implementation of hospital information systems and associated security controls in multi-hospital networks, including projects that involved thousands of users and a wide range of clinical departments.

Insights from the literature review were used to ensure that the architecture is aligned with current understanding of healthcare cyber risk and best practice. Experience from implementation projects was used to test and refine these ideas against operational realities, such as the constraints posed by legacy devices, contractual arrangements with vendors, and the need to keep clinical disruption to an acceptable minimum. The resulting architecture is therefore both evidence-informed and practice-tested, positioning it as a credible reference point for other organisations.

4. Healthcare Zero-Trust Resilience Architecture (HZTRA)

The HZTRA organises hospital cybersecurity around five integrated domains: identity and access management, network micro-segmentation, protection of medical devices and Internet of Medical Things assets, application-level security for clinical systems, and continuous monitoring with incident response. These domains span the hospital technology landscape, which typically includes core hospital information systems, electronic health record platforms, laboratory and radiology systems, connected bedside devices, and external telehealth services. By presenting these domains as parts of a single, coherent architecture, the HZTRA provides a shared mental model that can be used by technical and clinical stakeholders when planning cybersecurity improvements.

4.1 Identity and access management

Identity and access management is the foundation of the HZTRA. In a hospital setting, identities include clinicians, administrative staff, temporary workers, external vendors, service accounts, and, in some cases, patients accessing portals. A zero-trust approach requires that each identity is strongly verified, that access rights are minimised to what is necessary for the role, and that access decisions are continuously re-evaluated as context changes.

In the projects that informed this work, a central identity provider was integrated with core clinical systems using modern authentication standards. Multi-factor authentication was progressively rolled out for high-risk actions and remote access, while role- and attribute-based access control were used to align system access with clinical responsibilities. These patterns are captured in the HZTRA so that other organisations can reuse them when designing their own identity strategies.

4.2 Network micro-segmentation and secure zones

To limit lateral movement, the HZTRA divides the hospital network into logically separate security zones that reflect clinical and technical boundaries. Typical zones include core clinical systems, medical device networks, administrative systems, public or guest networks, and external connectivity to partners and cloud services. Micro-segmentation is applied within and between these zones using software-defined networking and fine-grained access policies, so that compromise of one device or segment does not automatically provide a path to critical systems.

In real deployments, this zoning approach has been used to isolate high-risk or legacy components while maintaining necessary data flows to clinical applications. Access between zones is mediated by policy enforcement points that evaluate identity, device posture, and requested service before allowing communication. These decisions can be tuned over time as monitoring data reveals typical and atypical patterns of use.

4.3 Medical device and Internet of Medical Things protection

Connected medical devices and other Internet of Medical Things assets are a distinctive feature of hospital environments and a major source of cyber risk. Many devices run legacy operating systems, are difficult to patch, or are supported under strict vendor contracts that limit direct security changes. The HZTRA treats these devices as high-value, high-risk assets that must be isolated, monitored, and mediated through secure gateways.

Practical implementations influenced the model's emphasis on accurate device inventories, behaviour profiling, and dedicated network zones for medical equipment. Where possible, device traffic is proxied through gateways that can enforce encryption, inspect traffic, and apply additional authentication. These measures have been used in production to reduce exposure without interrupting clinical use, and the architecture encourages other organisations to follow a similar pattern.

4.4 Application-level security for clinical systems

At the application layer, the HZTRA emphasises secure design and configuration of core clinical platforms such as electronic health records, laboratory information systems, radiology information systems, and clinical portals. Zero-trust principles are applied by aligning application access controls with central identity services, enforcing least-privilege roles,

and limiting direct database access. Application programming interfaces that expose clinical data to external systems or digital health applications are protected by strong authentication, authorisation, and rate limiting.

These practices were refined through experience with implementations in which inconsistent application configurations and ad hoc interfaces created avoidable risk. By codifying preferred patterns in the architecture, the article offers other hospitals a starting point that reflects lessons already learned the hard way.

4.5 Continuous monitoring and incident response

Continuous monitoring and effective incident response are essential to operationalising zero-trust in a hospital. The HZTRA aggregates telemetry from identities, endpoints, medical devices, network segments, and applications into a central security operations capability. Correlation and analytics across these data sources support detection of suspicious patterns such as unusual login locations, anomalous device traffic, or attempts to access restricted clinical data.

In the environments that inspired this model, incident response procedures were designed with clinical safety in mind, balancing the need to contain attacks with the imperative to maintain critical patient care services. Playbooks describe how to isolate affected segments, switch to contingency workflows, and communicate with clinical and executive stakeholders. The architecture preserves these patterns so that other organisations can adapt them rather than starting from scratch.

4.6 Alignment with hospital workflows

Finally, the HZTRA is designed to align security controls with real-world hospital workflows rather than imposing purely technical constraints. Access policies and segmentation boundaries are mapped to clinical pathways such as admissions, surgery, intensive care, and outpatient care, so that clinicians can perform necessary tasks without unnecessary friction. Engagement with clinical leaders and operational staff is assumed from the outset to ensure that zero-trust measures support, rather than hinder, safe and efficient care delivery.

This focus on clinical usability distinguishes the architecture from many purely technical models and has been critical to securing buy-in from stakeholders during actual implementation projects. It also increases the likelihood that organisations that adopt the HZTRA will sustain their security posture over time.

5. Discussion

The HZTRA demonstrates how zero-trust principles can be translated into a concrete, hospital-focused architecture that accounts for both technical and organisational realities. By documenting a model that has already guided real implementations, the article provides the broader community with a tested blueprint rather than a purely theoretical construct. This makes it easier for other hospitals to accelerate their cybersecurity programmes and avoid repeating avoidable mistakes.

From an impact perspective, the architecture also creates a reference point that vendors and consulting partners can align with when proposing solutions to healthcare providers. A shared framework helps ensure that products and services address genuine needs, such as device visibility or segmentation, rather than introducing isolated tools that are difficult to integrate. As the HZTRA is adopted, critiqued, and extended, it can serve as a foundation for more standardised approaches to hospital cybersecurity across regions and health systems.

For individual practitioners, including the architect who led this work, the HZTRA provides a clear narrative of contribution: it encapsulates design decisions taken in complex projects and offers them in a form that others can reuse. Evidence of external uptake—such as citations, independent implementations, and endorsements from hospital leaders—can in turn be used to demonstrate that the contribution is both original and of significance to the field of healthcare cybersecurity.

6. Conclusion

Cyberattacks on hospitals are a persistent threat to the continuity and safety of care, and existing perimeter-based defences have repeatedly proven insufficient. Zero-trust principles offer a compelling alternative, but without sector-specific guidance they can be difficult to translate into practice. The Healthcare Zero-Trust Resilience Architecture presented here addresses this gap by providing a structured, practitioner-led model tailored to the realities of hospital environments.

By organising security capabilities into integrated domains and aligning them with clinical workflows, the HZTRA offers a practical blueprint for hospitals seeking to strengthen their cyber resilience without compromising usability. Its roots in

real implementation projects give it credibility with technical and clinical stakeholders alike and create a pathway for broader adoption. As more organisations adapt and build on this architecture, its influence on healthcare cybersecurity practice can be measured and documented, providing concrete evidence of its contribution to the field.

Future work will involve partnering with hospitals and health systems to implement the HZTRA in diverse contexts, measure its impact on risk and operational performance, and refine its components based on empirical evidence. Such collaboration will be essential to establishing zero-trust architectures as a standard of practice in healthcare and to demonstrating, through independent validation, the value of practitioner-led contributions like the HZTRA.