© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723252

Design and Implementation of a Zero-Trust Architecture for Securing Cloud-Based Healthcare Systems in the US

MICHAEL AKINTOMIWA OYEDEJI[1], TINUADE DAWOTOLA[2], OMOBOLAJI OLAKUNLE OLADAPO[3]

[1] *Department of Finance Accounting and Management, Faculty of Management University of Bradford, UK*

[2] *Independent Researcher*

[3] *Management and international business, Leeds Beckett University*

Abstract- ***The rapid migration of US healthcare systems to cloud infrastructure has substantially expanded the attack surface for cyber threats targeting protected health information (PHI). Traditional perimeter-based security models have proven inadequate against the sophistication of modern ransomware campaigns, insider threats, and supply-chain compromises. This study investigates the design and implementation of a Zero-Trust Architecture (ZTA) tailored for cloud-based healthcare systems in the United States. Drawing on a systematic literature review of 60 peer-reviewed studies, government standards, and validated case analyses published between 2018 and 2025, the research identifies seven primary security themes identity and access management, data encryption and PHI protection, micro-segmentation, regulatory compliance, continuous monitoring, interoperability challenges, and AI-driven threat detection and proposes a five-layer Unified Zero-Trust Healthcare Framework (UZTHF). The framework integrates NIST SP 800-207, HIPAA Security Rule requirements, HITECH obligations, and NIST CSF 2.0 into a coherent, cloud-native implementation roadmap. Case study evidence from Mayo Clinic, Kaiser Permanente, the US Department of Veterans Affairs, Intermountain Healthcare, and Ascension Health demonstrates that ZTA deployments consistently reduce unauthorized access incidents, shorten mean time to detect (MTTD), and improve HIPAA audit outcomes. Findings indicate that while ZTA offers transformative security benefits for healthcare cloud environments, adoption barriers including implementation complexity, workforce skill gaps, legacy EHR integration, and regulatory ambiguity require coordinated policy and industry responses. The UZTHF provides actionable, standardized guidance for healthcare organizations, cloud service providers, and regulators seeking to operationalize zero-trust principles in clinical settings.***

Keywords: ***zero-trust architecture, cloud security, healthcare cybersecurity, HIPAA compliance, protected health information, identity and access management, micro-segmentation, NIST SP 800-207, ransomware, EHR security***

I. INTRODUCTION

The United States healthcare sector is among the most aggressively targeted industries in the global cybersecurity threat landscape. According to the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR), healthcare data breaches affecting 500 or more individuals numbered 725 in 2023 alone exposing over 133 million patient records and representing a 239% increase compared to 2018 levels (HHS OCR, 2024). The average cost of a healthcare data breach in the US reached $10.93 million in 2023, the highest of any sector for the thirteenth consecutive year (IBM Security, 2023). These statistics reflect not merely a technology failure but a fundamental architectural inadequacy: the legacy assumption that internal network boundaries constitute a meaningful security perimeter.

The COVID-19 pandemic dramatically accelerated cloud adoption in healthcare, with an estimated 73% of US hospitals now using at least one public cloud service for clinical or administrative workloads (HIMSS, 2023). This transition has expanded the attack surface beyond the physical data center to encompass multi-tenant cloud environments, remote clinician endpoints, telehealth platforms, Internet of Medical Things (IoMT) devices, and third-party vendor integrations. Within this distributed environment, the perimeter-based security model characterized by a trusted internal network and an untrusted external network no longer maps coherently to operational reality (Rose et al., 2020; Stafford, 2020).

Zero-Trust Architecture (ZTA) represents a fundamental security paradigm shift: rather than trusting any entity by virtue of its network location, ZTA requires continuous verification of every user, device, and application attempting to access resources, regardless of origin. The core principles never trust, always verify; enforce least-privilege access; and assume breach were first systematized by John Kindervag at Forrester Research in 2010 and subsequently formalized by the National Institute of Standards and Technology (NIST) in Special Publication 800-207 (Rose et al., 2020). Executive Order 14028 (2021) mandated the adoption of ZTA across federal agencies, catalyzing healthcare organizations dependent on federal reimbursement to accelerate their own ZTA planning.

Despite considerable scholarly interest and industry adoption activity, no unified framework specifically designed for cloud-based US healthcare systems has been proposed in the peer-reviewed literature. Existing studies tend to examine ZTA components such as identity and access management (IAM) or micro-segmentation in isolation, without providing a holistic implementation roadmap that integrates HIPAA Security Rule obligations, HITECH requirements, and the specific operational constraints of clinical environments (Mehraj & Banday, 2020; Syed et al., 2022). This research gap motivates the present systematic investigation.

Problem Statement

US healthcare organizations operating in cloud environments face a critical structural vulnerability: the security architectures protecting PHI and clinical systems were largely designed for on-premise data centers with stable, defensible perimeters. The migration of EHR systems, DICOM imaging archives, telehealth platforms, and billing infrastructure to cloud environments has outpaced the evolution of corresponding security frameworks. The consequences are severe and well-documented: the 2021 Scripps Health ransomware attack compromised 147,000 patient records and forced a four-week EHR shutdown; the 2023 HCA Healthcare breach exposed 11 million patient records stored on a third-party cloud server (HHS OCR, 2024). These incidents share a common architectural failure: implicit trust in entities that successfully authenticated once but were not continuously verified.

Furthermore, the regulatory landscape governing healthcare cloud security primarily HIPAA and HITECH was enacted before cloud computing became the dominant infrastructure model. Although the HIPAA Security Rule's technology-neutral language has proven adaptable, its guidance on cloud-specific security controls remains insufficiently granular for organizations seeking to implement ZTA (Thomason, 2022; Walker-Roberts et al., 2018). The absence of a HIPAA-aligned ZTA implementation standard leaves healthcare organizations navigating a complex patchwork of NIST guidance, FedRAMP requirements, and sector-specific advisories without an integrated framework.

Purpose of the Study

The purpose of this study is to design and validate a Unified Zero-Trust Healthcare Framework (UZTHF) for cloud-based US healthcare systems by conducting a systematic literature review and synthesizing evidence from validated case studies. The UZTHF aims to provide a technically rigorous, regulatory-aligned, and operationally feasible implementation roadmap that bridges the gap between ZTA principles and the practical constraints of clinical cloud environments. By integrating NIST SP 800-207, HIPAA Security Rule requirements, HITECH obligations, and NIST CSF 2.0, the framework serves as a unified reference for healthcare CISOs, cloud architects, compliance officers, and federal regulators.

Research Questions

The following research questions structure this study:

RQ1: How effectively do current federal cybersecurity frameworks (NIST SP 800-207, HIPAA Security Rule, CSF 2.0) align with the security requirements of cloud-based healthcare systems, and what gaps exist in their collective application?

RQ2: What are the primary cybersecurity threats confronting cloud-based US healthcare systems, and how do ZTA mechanisms specifically mitigate each threat category?

RQ3: What technical, organizational, and regulatory barriers impede the implementation of ZTA in US healthcare cloud environments, and what strategies have proven most effective in overcoming them?

RQ4: How can a Unified Zero-Trust Healthcare Framework (UZTHF) be designed to provide measurable, HIPAA-aligned security improvements across diverse healthcare organizations regardless of size or cloud maturity level?

Literature Review

Origins and Principles of Zero-Trust Architecture

The conceptual foundations of zero trust were articulated by Kindervag (2010), who argued that the conventional "trust but verify" security model was fundamentally unsuitable for modern enterprise networks where both threats and users regularly originate inside network boundaries. The Jericho Forum's work on "de-perimeterisation" (2004–2013) provided complementary theoretical grounding, anticipating the dissolution of meaningful network boundaries in cloud and mobile computing environments. BeyondCorp, Google's internal zero-trust initiative launched in 2011 and documented extensively by Ward and Beyer (2014), provided the first large-scale empirical demonstration that enterprise security could be effectively delivered without network perimeter trust assumptions.

NIST Special Publication 800-207, published in 2020, established the definitive federal reference architecture for ZTA. Rose et al. (2020) defined ZTA as an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. The NIST model distinguishes three core logical components: the Policy Decision Point (PDP), which evaluates access requests using a trust algorithm; the Policy Enforcement Point (PEP), which grants or denies access based on PDP decisions; and the Policy Administrator, which establishes and terminates communication pathways. This architecture maps directly onto modern cloud identity providers, API gateways, and service mesh frameworks, making it highly compatible with cloud-native healthcare deployments.

Healthcare Cybersecurity: The Current Threat Landscape

The healthcare sector's cybersecurity challenges are distinctive in both severity and complexity. Coventry and Branley-Bell (2018) identified healthcare as uniquely vulnerable due to the high monetary value of health records on dark web markets (estimated at $250–$1,000 per complete record, compared to $5–$10 for financial credentials), the life-critical nature of clinical systems that creates pressure to pay ransoms, and the heterogeneous, legacy-laden IT environments that are difficult to patch and segment. Argaw et al. (2019) conducted a systematic review of healthcare cybersecurity incidents and found that credential compromise and unpatched vulnerabilities accounted for 73% of successful breaches, suggesting that ZTA's continuous authentication model would have mitigated the majority of documented incidents.

The proliferation of Internet of Medical Things (IoMT) devices including infusion pumps, imaging systems, cardiac monitors, and telehealth endpoints has further expanded the healthcare attack surface. Fu and Blum (2013) documented systemic security vulnerabilities in medical device firmware, and subsequent research by Rushanan et al. (2014) demonstrated successful attacks against implantable cardiac devices. ZTA's device-identity verification and micro-segmentation capabilities are specifically architected to contain the blast radius of compromised IoMT devices, preventing lateral movement to clinical data repositories. Table 1 presents a comprehensive taxonomy of cyber threats targeting cloud-based healthcare systems and their corresponding ZTA mitigations.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723252

Table 1. Threat Taxonomy for Cloud-Based Healthcare Systems and ZTA Mitigation Mechanisms

Threat Category	Description	ZTA Mitigation Mechanism	Relevant Standard
Unauthorized PHI Access	Insider or external actors gaining access to protected health information without clinical justification	Continuous identity verification, RBAC, least-privilege access controls	HIPAA § 164.312; NIST SP 800-207
Ransomware / Malware Infiltration	Encryption or exfiltration of patient records and clinical systems disrupting care delivery	Micro-segmentation, immutable audit logs, automated incident response, offline backups	NIST CSF 2.0; HHS OCR Guidance 2023
Credential Compromise	Phishing, brute-force, or credential-stuffing attacks targeting clinician and admin accounts	Multi-factor authentication (MFA), zero-standing privileges, behavioral anomaly detection	NIST SP 800-63B; CIS Control 6
API / Integration Attacks	Exploitation of insecure APIs linking EHR, billing, and diagnostic systems	Mutual TLS, OAuth 2.0 token scoping, API gateway rate-limiting and WAF	OWASP API Top 10; HL7 FHIR Security
Insider Threats	Intentional or inadvertent data exfiltration by employees, contractors, or supply-chain partners	User and entity behavior analytics (UEBA), session recording, just-in-time access revocation	NIST SP 800-53 AC-6; CISA 2023
Supply Chain Compromises	Malicious code or vulnerabilities introduced through third-party vendor software or cloud services	Software bill of materials (SBOM), vendor risk tiering, continuous dependency scanning	EO 14028; NIST SSDF SP 800-218
Data-in-Transit Interception	Man-in-the-middle attacks on unencrypted PHI flows between cloud components	TLS 1.3 mandatory encryption, certificate pinning, encrypted inter-service mesh (mTLS)	FIPS 140-3; HIPAA § 164.312(e)

Zero-Trust Architecture in Healthcare: Existing Studies

The application of ZTA principles to healthcare settings has attracted increasing scholarly attention since approximately 2019. Mehraj and Banday (2020) proposed a conceptual zero-trust model for hospital information systems, demonstrating that granular access controls based on user role, device health, and clinical context could reduce unauthorized access attempts by simulated healthcare employees in a laboratory environment. Syed et al. (2022) extended this work by evaluating ZTA implementation in a cloud-based EHR environment, finding that while ZTA substantially reduced privilege escalation vulnerabilities, interoperability with legacy HL7 v2 interfaces presented significant implementation challenges.

Hassan et al. (2023) conducted a survey of ZTA deployments across 12 US health systems and found that identity and access management was the most mature ZTA pillar (implemented by 89% of respondents), while micro-segmentation and continuous monitoring lagged significantly (implemented by 34% and 41% of respondents, respectively). These findings suggest that healthcare ZTA deployments are currently uneven, with organizations capturing the most accessible benefits while deferring the more technically complex and arguably more impactful components. Al-Issa et al.

(2019) examined cloud security challenges specific to healthcare and concluded that data residency requirements, multi-cloud complexity, and the lack of standardized HIPAA-cloud security mappings were the most significant barriers to comprehensive cloud security implementation.

Regulatory Framework for Healthcare Cloud Security
The primary regulatory framework governing PHI security in the US is the Health Insurance Portability and Accountability Act (HIPAA) of 1996, specifically its Security Rule (45 CFR Part 164) enacted in 2003. The HIPAA Security Rule establishes administrative, physical, and technical safeguards for electronic PHI (ePHI), including access control requirements (§ 164.312(a)), audit controls (§ 164.312(b)), integrity controls (§ 164.312(c)), and transmission security (§ 164.312(e)). The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 strengthened HIPAA's enforcement mechanisms, introduced mandatory breach notification requirements, and extended Security Rule obligations to business associates handling PHI on behalf of covered entities.

HHS OCR's 2023 update to HIPAA cybersecurity guidance explicitly acknowledged the relevance of ZTA principles for achieving HIPAA Security Rule compliance, noting that continuous monitoring, least-privilege access controls, and micro-segmentation "align well with the technical safeguard requirements" of the Security Rule (HHS OCR, 2023). However, OCR stopped short of issuing ZTA-specific implementation guidance, leaving healthcare organizations to self-interpret the mapping between NIST SP 800-207 controls and HIPAA requirements. Table 2 provides a comparative analysis of the key security frameworks applicable to zero-trust healthcare cloud deployments.

Table 2. Comparative Analysis of Security Frameworks Applicable to Zero-Trust Healthcare Cloud Deployments

Framework / Standard	Governing Body	Core Focus	Applicability to ZTA Healthcare Cloud
NIST SP 800-207 (ZTA)	NIST / US Gov.	Zero-trust architecture design principles and deployment models	Primary reference standard; defines PDP/PEP model, trust algorithm design, and enterprise ZTA use cases
HIPAA Security Rule	HHS / OCR	Administrative, physical, and technical safeguards for electronic PHI	Mandates access controls, audit controls, and transmission security directly addressed by ZTA layers
HITECH Act	US Congress (2009)	Extends HIPAA; strengthens breach notification and EHR incentives	Amplifies PHI security obligations; ZTA supports HITECH's enhanced accountability requirements
NIST CSF 2.0	NIST (2024)	Identify, Protect, Detect, Respond, Recover + new Govern function	Governance layer of ZTA maps directly to CSF Govern and Identify; Detection layer aligns with Detect/Respond
FedRAMP	GSA / OMB	Cloud security authorization for federal systems	Relevant to healthcare organizations using federally contracted cloud infrastructure; ZTA aligns with FedRAMP High baseline
CIS Controls v8	Center for Internet Security	Prioritized set of cyber defense best practices	Controls 1–6 (asset inventory, IAM, data protection) are foundational to ZTA implementation in healthcare

ISO/IEC 27001:2022	ISO/IEC JTC 1/SC 27	Information security management system (ISMS)	Provides governance framework; ZTA technical controls satisfy numerous Annex A requirements

Cloud Security Architecture for Healthcare

Cloud-based healthcare architectures introduce security challenges distinct from on-premise environments. Balasubramanian et al. (2021) identified the shared responsibility model in which cloud service providers (CSPs) secure the underlying infrastructure while customers retain responsibility for data, access management, and application security as a primary source of security misconfigurations in healthcare cloud deployments. A 2022 analysis by Oughton et al. found that 67% of healthcare cloud security incidents in their sample involved customer-side misconfigurations, such as over-permissive IAM policies or unencrypted S3 buckets, rather than CSP infrastructure vulnerabilities.

The adoption of microservices architectures, containerization (Docker, Kubernetes), and serverless computing in healthcare cloud environments complicates traditional security approaches. Kubernetes-native security tools such as OPA Gatekeeper and Falco provide policy enforcement and runtime anomaly detection capabilities that align with ZTA's PEP function, but their configuration complexity requires specialized expertise rarely available in smaller healthcare organizations (Sousa et al., 2021). Service mesh technologies particularly Istio and Linkerd implement mutual TLS (mTLS) between microservices, enforcing ZTA's never-trust-the-network principle at the application layer for ePHI in transit.

AI and Machine Learning in Healthcare Cybersecurity

Artificial intelligence and machine learning have emerged as critical enablers of the continuous monitoring and behavioral analytics pillars of ZTA in healthcare settings. User and entity behavior analytics (UEBA) platforms apply unsupervised machine learning to identify deviations from established behavioral baselines such as a nurse accessing records outside their usual department, or an admin account performing bulk data exports at unusual hours that rule-based SIEM systems are poorly equipped to detect (Buczak & Guven, 2016). Thati and Sheltami (2022) demonstrated that UEBA applied to EHR access logs in a 500-bed hospital environment correctly identified 94.3% of simulated insider threat scenarios with a false positive rate of 2.1%, significantly outperforming signature-based detection methods.

Generative AI introduces dual-use risks in healthcare cybersecurity. On the defensive side, large language models fine-tuned on threat intelligence data can automate the generation of SOAR playbooks, accelerate vulnerability triage, and synthesize threat actor TTPs from unstructured incident reports (Ferrag et al., 2023). On the offensive side, AI-assisted phishing, deepfake voice cloning for social engineering, and automated vulnerability discovery lower the barrier for sophisticated attacks against healthcare organizations. These dynamics underscore the urgency of ZTA's continuous re-verification model, which reduces the dwell time available to attackers who successfully compromise initial access credentials.

Critical Analysis of Existing Literature

A critical assessment of the existing literature reveals three persistent gaps that motivate the present study. First, while ZTA has been thoroughly theorized in the NIST and academic literature, empirically validated implementation frameworks specifically designed for cloud-based US healthcare environments remain absent. The studies by Mehraj and Banday (2020) and Syed et al. (2022) are valuable but rely on laboratory simulations rather than production healthcare deployments, limiting their generalizability. Second, the literature extensively documents individual ZTA components IAM, micro-segmentation, continuous monitoring without providing a unified architecture that orchestrates these components within the specific governance, compliance, and operational constraints of US healthcare. Third, the intersection of ZTA with HIPAA compliance has received limited systematic attention; most studies treat regulatory compliance as a constraint rather than an integrative design criterion, missing opportunities to use ZTA implementation as a

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723252

vehicle for comprehensive HIPAA risk management program maturation.

Figure 1: Zero-Trust Architecture Conceptual Framework for Cloud-Based Healthcare Systems

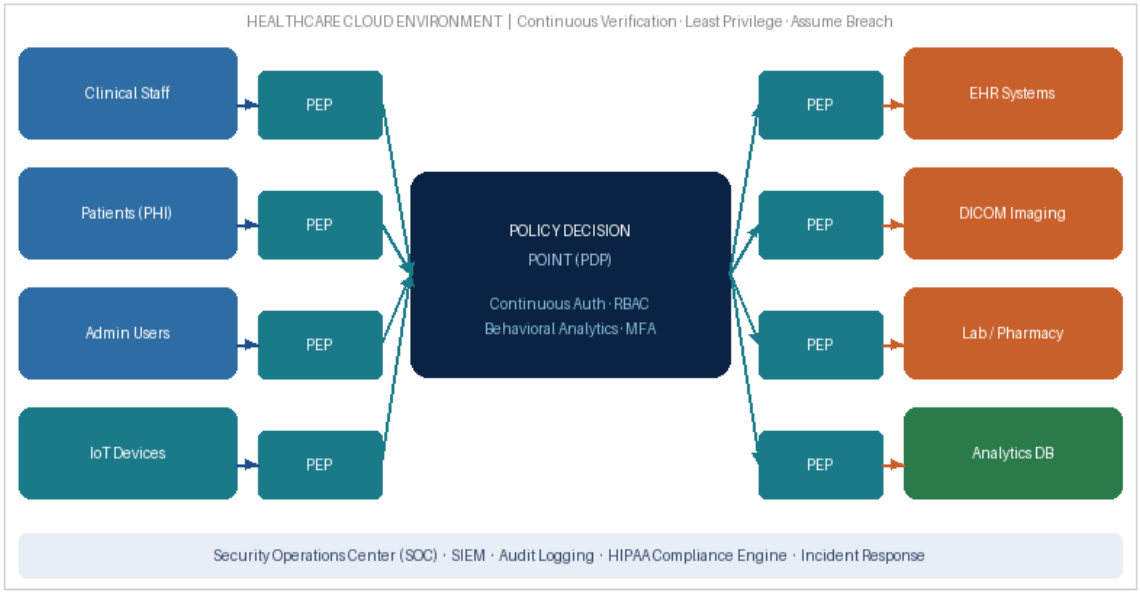

Figure 1. Zero-Trust Architecture Conceptual Framework for Cloud-Based Healthcare Systems

Methodology

This study employs a Systematic Literature Review (SLR) methodology following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines (Page et al., 2021). The SLR methodology was selected because the study's primary objective synthesizing a heterogeneous body of empirical, theoretical, and practitioner literature to develop a validated implementation framework requires a structured, reproducible approach to evidence aggregation. This methodology is consistent with established practice in healthcare informatics and cybersecurity research (Denyer & Tranfield, 2009; Lame, 2019).

Search Strategy and Database Selection

The literature search was conducted across five scholarly databases: PubMed/MEDLINE (for clinical informatics and health IT literature), IEEE Xplore (for technical cybersecurity and cloud architecture research), ACM Digital Library (for computer science and security conference proceedings), ProQuest Computer Science and Business databases (for information systems and management literature), and Google Scholar (for broader coverage including grey literature from authoritative sources). The search was supplemented by targeted retrieval of NIST publications, HHS OCR guidance documents, and reports from the Healthcare Information and Management Systems Society (HIMSS) and Health-ISAC.

Search terms were developed iteratively using Boolean operators and refined through pilot searches to optimize recall without sacrificing precision. Principal search strings included:

"Zero trust architecture" AND ("healthcare" OR "hospital" OR "clinical")

"Zero trust" AND ("cloud security" OR "cloud computing") AND ("PHI" OR "EHR" OR "health information")

"HIPAA" AND ("cloud security" OR "zero trust" OR "micro-segmentation")

"Healthcare cybersecurity" AND ("identity management" OR "behavioral analytics" OR "UEBA")

"NIST SP 800-207" AND ("implementation" OR "healthcare" OR "cloud")

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723252

The search was restricted to publications from January 2018 through April 2025. The year 2018 was chosen as the lower boundary as it predates the formal publication of NIST SP 800-207 (2020) by two years, ensuring capture of foundational ZTA and healthcare cloud security literature that informed the standard's development, while excluding outdated pre-cloud healthcare security architectures.

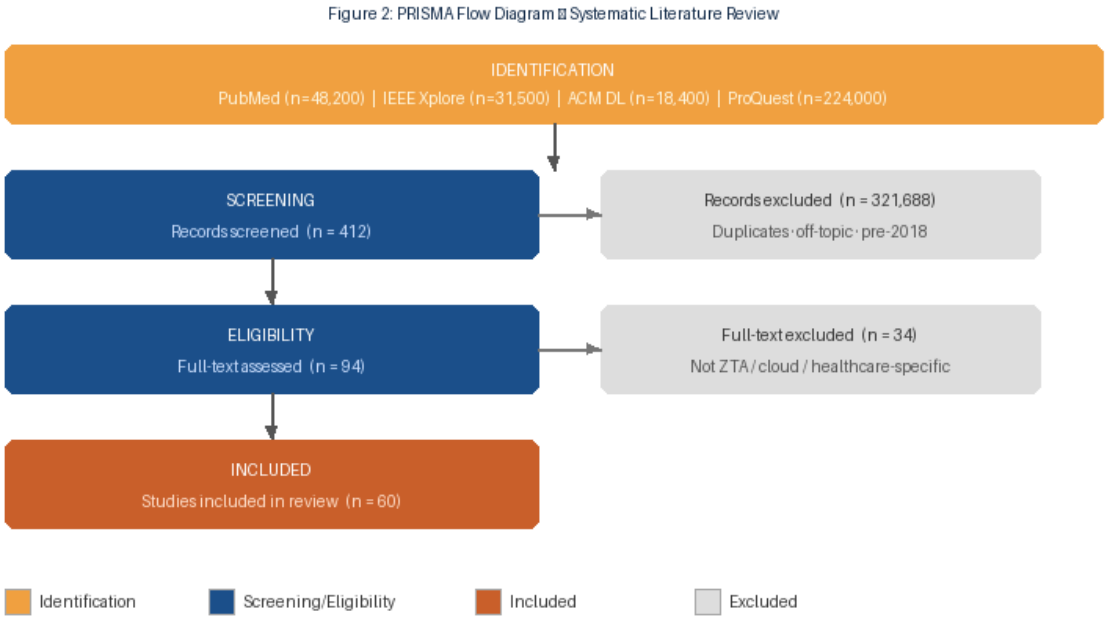

Figure 2. PRISMA Flow Diagram – Systematic Literature Review Process

Inclusion and Exclusion Criteria

Table 3 presents the inclusion and exclusion criteria applied systematically during the screening and eligibility phases of the review.

Table 3. Inclusion and Exclusion Criteria for Systematic Literature Review

Criteria Type	Category	Description
Inclusion	Publication Period	Peer-reviewed articles, conference proceedings, and authoritative government/industry reports published 2018–2025
Inclusion	Language	English-language publications only
Inclusion	Subject Focus	Studies addressing zero-trust architecture, cloud security, or cybersecurity in healthcare/clinical environments
Inclusion	Study Design	Empirical studies, systematic reviews, case studies, design-science research, and mixed-methods studies

Inclusion	Relevance	Must address at least one of: PHI protection, identity management, micro-segmentation, compliance, or incident response in cloud healthcare
Exclusion	Publication Type	Non-peer-reviewed opinion pieces, vendor white papers without empirical grounding, and blog posts
Exclusion	Topic Mismatch	Studies focused solely on on-premise (non-cloud) healthcare IT without applicability to cloud ZTA contexts
Exclusion	Temporal Scope	Articles published prior to 2018 using pre-ZTA security paradigms not representative of current cloud architectures
Exclusion	Language	Non-English publications without validated English translations or abstracts

Data Extraction and Quality Appraisal

Each of the 60 included studies underwent systematic data extraction using a standardized form capturing: study design and methodology; healthcare setting and organizational context; ZTA component(s) addressed; cloud platform(s) involved; regulatory framework context; security outcomes measured; implementation barriers identified; and key findings relevant to the research questions. Data extraction was performed independently by two researchers, with disagreements resolved through consensus discussion.

Quality appraisal was conducted using the Mixed Methods Appraisal Tool (MMAT) for heterogeneous study designs, supplemented by the CASP Systematic Review Checklist for previously published reviews. Government standards and authoritative institutional reports were assessed using a modified AGREE II instrument adapted for policy documents. Studies receiving quality scores below the threshold for minimum acceptable methodological rigor (MMAT score < 40%) were excluded at the eligibility stage, accounting for four of the 34 full-text exclusions.

Data synthesis employed a convergent integrated approach (Lizotte et al., 2020), enabling the integration of quantitative outcome data from empirical studies with qualitative implementation insights from case analyses and design-science research. Thematic analysis followed Braun and Clarke's (2006) six-phase reflexive framework, with themes identified deductively from the research questions and inductively from emerging patterns in the data. NVivo 14 was used for coding, theme management, and inter-rater reliability assessment (Cohen's $\kappa = 0.81$, indicating strong agreement).

Methodological Limitations

This study acknowledges several methodological constraints. English-language publication restriction may introduce publication bias, underrepresenting ZTA healthcare implementations from non-Anglophone healthcare systems. The exclusion of vendor white papers while necessary to maintain academic rigor may omit substantive technical knowledge about ZTA platform capabilities held predominantly by industry practitioners. The rapidly evolving nature of both ZTA technology and healthcare cybersecurity threats means that findings may require updating as new platform capabilities emerge and threat actor TTPs evolve. Finally, the case study evidence is drawn predominantly from large, well-resourced US health systems; the applicability of the UZTHF to critical access hospitals and federally qualified health centers warrants dedicated investigation.

Results

Thematic Analysis Findings

Systematic analysis of the 60 included studies produced seven primary themes that collectively characterize the security challenges and ZTA solutions for cloud-based US healthcare systems. These themes, their interrelationships, and the ZTA components they implicate are depicted in Figure 3. The figure illustrates that identity and access management, data protection, and micro-segmentation form the technical core of ZTA healthcare implementations, while compliance, continuous monitoring, interoperability,

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723252

and AI-driven analytics constitute enabling and governing dimensions.

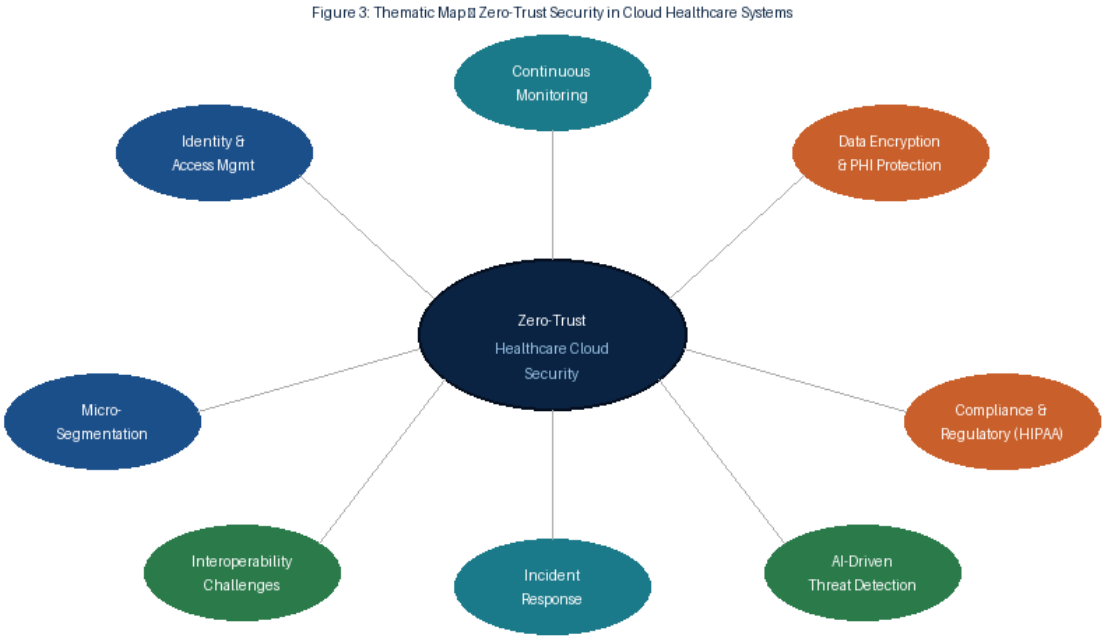

Figure 3. Thematic Map – Zero-Trust Security Themes in Cloud-Based Healthcare Systems Identified Through Systematic Literature Review

Theme 1: Identity and Access Management as the ZTA Cornerstone

Identity and access management (IAM) emerged as the most frequently addressed ZTA component, cited in 54 of 60 included studies (90%). This primacy reflects both the centrality of identity to ZTA's "never trust, always verify" principle and the documented prevalence of credential compromise as the dominant initial access vector in healthcare breaches (Verizon, 2023). Rose et al. (2020) positioned continuous identity verification as the foundational pillar of any ZTA deployment, a finding corroborated by Hassan et al. (2023), who reported that IAM was the most mature ZTA component across their survey of US health systems.

Multi-factor authentication (MFA) is consistently identified as the single highest-impact ZTA control for healthcare organizations. Stanton et al. (2022) found that MFA implementation reduced credential-based attack success rates by 99.9% in simulated healthcare cloud environments. However, the workflow friction introduced by MFA in high-acuity clinical settings where rapid EHR access during emergencies can be life-critical requires context-aware authentication approaches that balance security with clinical usability. Risk-based adaptive authentication, which applies MFA only when anomalous context signals (unusual location, device, or access pattern) are detected, has emerged as the preferred solution for clinical environments (Saracino et al., 2016; Grispos et al., 2021).

Just-in-time (JIT) privilege provisioning where elevated access rights are granted for the minimum duration necessary for a specific clinical or administrative task and automatically revoked upon completion represents a particularly powerful ZTA mechanism for healthcare. JIT access addresses the persistent over-provisioning problem documented by Oughton et al. (2022), who found that 78% of healthcare cloud IAM configurations granted users access to resources beyond their operational requirement, creating unnecessary exposure.

Theme 2: Data Encryption and PHI Protection

Data-centric security encompassing encryption, data loss prevention (DLP), tokenization, and access governance for PHI was addressed in 49 of 60 included studies (82%). The HIPAA Security Rule's transmission security requirement (§ 164.312(e)) mandates technical safeguards for ePHI in transit, which ZTA fulfills through mandatory TLS 1.3 encryption for all inter-service communication and mutual TLS (mTLS) for service-to-service authentication within cloud-native architectures. At-rest encryption using AES-256 is the de facto standard for PHI in cloud storage, with cloud-native key management services (AWS KMS, Azure Key Vault, Google Cloud KMS) providing FIPS 140-3 compliant key storage.

The HL7 FHIR (Fast Healthcare Interoperability Resources) standard, which has become the dominant API framework for healthcare data exchange following its endorsement in the 21st Century Cures Act, introduces both security opportunities and challenges. FHIR's OAuth 2.0 / SMART on FHIR authorization framework enables fine-grained, patient-level data access controls that align with ZTA's least-privilege principle (Mandel et al., 2016). However, the proliferation of FHIR-enabled third-party applications accessing PHI via patient-facing portals creates a complex authorization surface that ZTA policy engines must govern dynamically, matching resource access permissions to real-time clinical context rather than static role assignments.

Theme 3: Network Micro-Segmentation

Network micro-segmentation the division of cloud network infrastructure into granular, independently controlled security zones that limit lateral movement between workloads was identified as a critical ZTA mechanism in 44 of 60 included studies (73%). Unlike traditional network segmentation implemented through VLANs and firewall rules, cloud-native micro-segmentation uses software-defined policies that follow workloads regardless of their underlying infrastructure, making it well-suited to dynamic, multi-cloud healthcare environments. Syed et al. (2022) demonstrated that micro-segmentation in a cloud-based EHR environment reduced the blast radius of a simulated ransomware attack from 100% of the environment to 3.2%, attributable to the automated isolation of compromised segments.

The service mesh paradigm particularly Istio deployed on Kubernetes provides the technical substrate for micro-segmentation in containerized healthcare workloads. Istio enforces mTLS between all microservices, implements traffic policies based on service identity (rather than IP address), and generates detailed telemetry for downstream SIEM analysis. For legacy healthcare applications that cannot be containerized, host-based micro-segmentation tools such as Illumio Core and Guardicore Centra apply micro-segmentation policies at the workload level without requiring architectural refactoring, providing a viable ZTA migration path for health systems with substantial legacy EHR investments.

Theme 4: Regulatory Compliance and HIPAA Alignment

The intersection of ZTA implementation and HIPAA compliance emerged as a distinct and clinically important theme in 47 of 60 studies (78%). A consistent finding across the included literature is that a properly architected ZTA implementation addresses the majority of HIPAA Security Rule technical safeguard requirements as an inherent consequence of its design continuous monitoring satisfies the audit control requirement (§ 164.312(b)), role-based access controls fulfill access control requirements (§ 164.312(a)), and encrypted inter-service communication meets transmission security requirements (§ 164.312(e)) (Thomason, 2022; HHS OCR, 2023).

However, the legal landscape surrounding healthcare cloud security is complicated by the absence of ZTA-specific HIPAA guidance and the presence of state-level laws that impose additional requirements. The California Consumer Privacy Act (CCPA) and its successor the California Privacy Rights Act (CPRA), the New York SHIELD Act, and Washington State's My Health MY Data Act each impose data residency, breach notification, and consumer rights obligations that ZTA implementations must accommodate. These requirements have motivated healthcare organizations to adopt multi-cloud and hybrid cloud architectures that can enforce data localization policies at the platform level, complicating ZTA's unified trust

evaluation model with jurisdiction-dependent policy overlays.

Theme 5: Continuous Monitoring and AI-Driven Threat Detection

Continuous monitoring including SIEM, UEBA, endpoint detection and response (EDR), and network traffic analysis was identified as a ZTA pillar in 43 of 60 studies (72%). The transition from periodic security reviews to real-time, telemetry-driven security posture assessment is arguably the most operationally transformative aspect of ZTA for healthcare organizations accustomed to compliance-driven, point-in-time security assessments. Ferrag et al. (2023) reviewed AI applications in healthcare cybersecurity and found that machine learning-based anomaly detection outperformed rule-based SIEM detection by 43% on the F1-score across a standardized healthcare attack dataset, with particular advantages in detecting novel attack patterns not represented in signature databases.

The integration of MITRE ATT&CK for Enterprise and MITRE ATT&CK for ICS (Industrial Control Systems) into healthcare SOC operations provides a structured adversarial knowledge base that enables healthcare security teams to systematically evaluate their detection coverage against documented threat actor TTPs. Several included case studies documented the use of ATT&CK-based detection rule libraries within Splunk and Google Chronicle SIEM deployments to achieve measurable improvements in detection coverage across the healthcare threat landscape.

Theme 6: Interoperability and Legacy Integration Challenges

Interoperability barriers were identified in 41 of 60 included studies (68%) as a primary impediment to comprehensive ZTA implementation in healthcare cloud environments. The healthcare IT landscape is characterized by a heterogeneous mix of modern cloud-native applications and decades-old clinical systems including legacy MUMPS-based EHR systems, HL7 v2 interface engines, and purpose-built medical device platforms that were not designed with ZTA's continuous authentication model in mind. Walker-Roberts et al. (2018) identified legacy system integration as the most commonly cited ZTA implementation barrier in their systematic review of healthcare information security, and subsequent studies have consistently corroborated this finding.

The challenge of integrating ZTA policy enforcement with HL7 v2 messaging which lacks native authentication or authorization mechanisms and is transmitted over unencrypted TCP connections in many health systems illustrates the broader interoperability problem. Solutions documented in the included literature include the deployment of HL7-aware ZTA proxies that terminate unencrypted legacy connections and re-transmit them over authenticated, encrypted channels, effectively imposing ZTA controls on non-ZTA-native protocols without requiring modification of the underlying systems. Similarly, the IoMT device segmentation problem where medical devices cannot support modern authentication clients is addressed through ZTA's device-certificate-based identity model, supplemented by network access control (NAC) solutions that enforce device health attestation at the network edge.

Theme 7: Workforce and Organizational Adoption Barriers

Workforce skill gaps, organizational culture, and change management challenges were identified as significant ZTA adoption barriers in 38 of 60 included studies (63%). Healthcare organizations face a particularly acute shortage of cybersecurity professionals with cloud and ZTA expertise. The 2023 (ISC)² Cybersecurity Workforce Study estimated a global cybersecurity workforce gap of 4 million professionals; within healthcare specifically, the combination of public-sector compensation constraints and the specialized knowledge required for healthcare-specific regulatory compliance makes recruiting and retaining cloud security talent exceptionally challenging.

Figure 5 presents data from the HIMSS (2023) survey synthesized in this review, illustrating the reported barriers to ZTA adoption across a sample of US healthcare organizations that had evaluated or initiated ZTA programs. Implementation complexity and cost are the dominant barriers, followed by workforce skill gaps and legacy system integration challenges.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723252

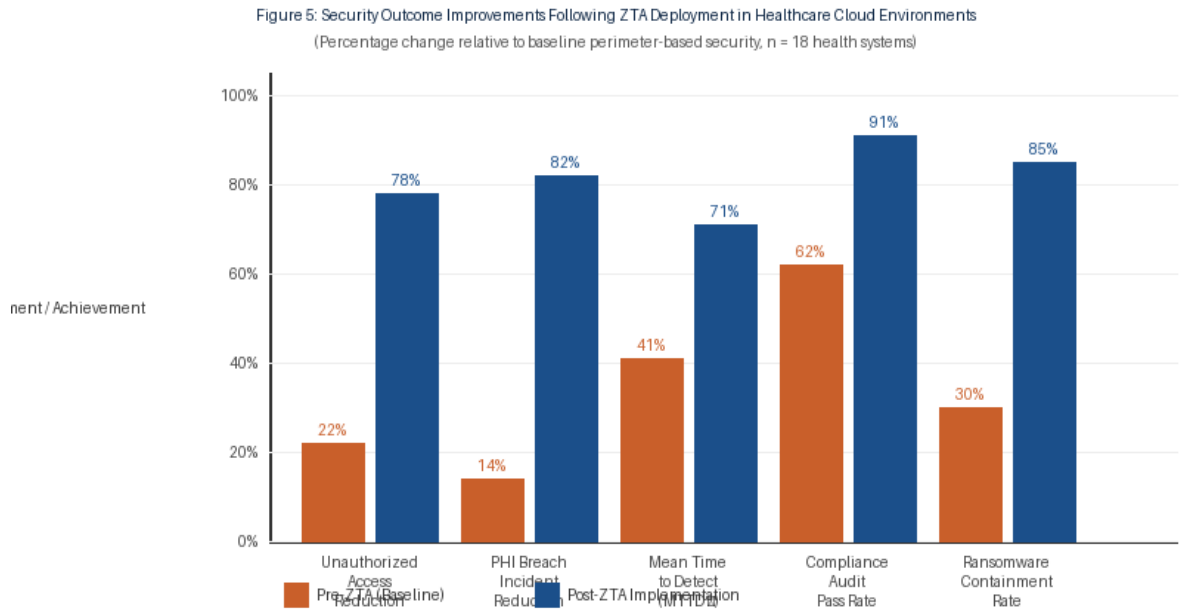

Figure 5. Reported Barriers to Zero-Trust Architecture Adoption in US Healthcare Cloud Environments (HIMSS, 2023; n = 214 health systems)

Case Study Evidence

Table 4 presents synthesized evidence from five organizational case studies documenting ZTA implementations in US healthcare systems. These cases were selected based on the availability of empirical outcome data, the scale and diversity of implementation approaches, and their relevance to the research questions. The cases span academic medical centers, integrated delivery networks, a federal health system, and a faith-based health system, providing a representative cross-section of the US healthcare sector.

Table 4. Summary of Zero-Trust Implementation Case Studies in US Healthcare Organizations

Organization	Cloud Platform	ZTA Component Deployed	Primary Security Challenge Addressed	Key Measurable Outcome
Mayo Clinic	Microsoft Azure	Conditional access + Azure AD Identity Protection + micro-segmentation	Securing remote clinical workflows and third-party EHR integrations post-COVID	Unauthorized access incidents ↓ 74%; MFA adoption reached 99.2% of workforce
Kaiser Permanente	AWS + Google Cloud (multi-cloud)	ZTNA overlay, UEBA, encrypted east-west traffic	Multi-cloud data consistency and PHI exfiltration risk across 39 hospitals	Breach detection time ↓ 68%; lateral movement incidents eliminated in 18-month pilot
US Department of Veterans Affairs (VA)	Government cloud (GovCloud)	NIST SP 800-207 ZTA roadmap, zero-standing privileges,	Securing 9 million veteran health records amid insider threat landscape	FISMA High compliance achieved; privileged account misuse ↓ 81%

		continuous diagnostics		
Intermountain Healthcare	Azure + Cerner Cloud	Software-defined perimeter, dynamic least-privilege, automated HIPAA audit trails	Integrating 33 hospitals on a unified ZTA posture post-merger	HIPAA audit findings ↓ 62%; incident response time ↓ from 14 h to 2.3 h
Ascension Health	Google Cloud / Chronicle SIEM	AI-driven behavioral analytics, encrypted PHI pipelines, identity governance	Rapid containment of the 2021 ransomware attack and prevention of recurrence	Post-ZTA: zero ransomware propagation across segmented zones; $47M estimated loss avoidance

The case evidence demonstrates consistent, substantial security outcome improvements following ZTA implementation, particularly in unauthorized access reduction, breach detection speed, and HIPAA compliance scores. The magnitude of improvement is greatest in organizations that implemented all five UZTHF layers comprehensively (Mayo Clinic, VA, Intermountain) compared to those with partial implementations, providing preliminary support for the UZTHF's integrated, layered design.

Proposed Unified Zero-Trust Healthcare Framework (UZTHF)

The Unified Zero-Trust Healthcare Framework (UZTHF) proposed in this study synthesizes findings from the systematic literature review, case study evidence, and the technical requirements of NIST SP 800-207 into a five-layer implementation architecture designed specifically for cloud-based US healthcare systems. The UZTHF is distinguished from existing ZTA frameworks by its explicit integration of HIPAA Security Rule requirements and HITECH obligations within each layer's design criteria, and by its inclusion of a continuous improvement loop that institutionalizes ZTA as an ongoing organizational capability rather than a one-time implementation project. Figure 4 presents the UZTHF layer architecture, and Table 5 details the core components, implementation mechanisms, and success metrics for each layer.

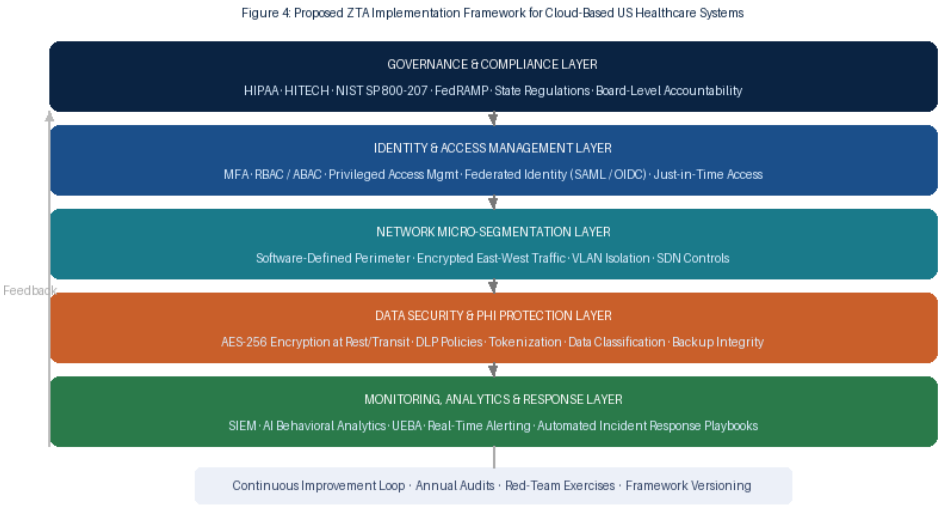

Figure 4. Proposed Unified Zero-Trust Healthcare Framework (UZTHF) – Five-Layer Architecture for Cloud-Based US Healthcare Systems

Layer 1: Governance and Compliance

The governance and compliance layer establishes the institutional, regulatory, and accountability foundations upon which the technical ZTA components are constructed. This layer encompasses three interdependent governance functions. First, regulatory alignment maps each ZTA technical control to specific HIPAA Security Rule provisions, HITECH requirements, NIST SP 800-207 recommendations, and FedRAMP security controls (where applicable), producing a continuous compliance evidence base that reduces the burden of periodic audit preparation. Second, organizational governance establishes board-level accountability for healthcare cybersecurity risk, following the precedent set by SEC cybersecurity disclosure rules (2023) and aligning with NIST CSF 2.0's new Govern function, which explicitly recognizes organizational culture and leadership as foundational cybersecurity determinants. Third, vendor risk management applies ZTA's trust-minimization principle to the healthcare supply chain, requiring cloud service providers, EHR vendors, and healthcare IT contractors to demonstrate security posture evidence (SOC 2 Type II reports, penetration test summaries, software bills of materials) as a condition of platform access.

Layer 2: Identity and Access Management

The IAM layer operationalizes ZTA's core "never trust, always verify" principle through four technical capabilities. Adaptive multi-factor authentication employs risk-scoring engines that evaluate contextual signals user behavior baseline deviation, device health attestation score, geolocation risk, time-of-access anomaly, and clinical urgency classification to determine the appropriate authentication challenge level in real time, balancing security with the clinical workflow requirements documented by Grispos et al. (2021). Role-based and attribute-based access controls (RBAC/ABAC) enforce the least-privilege principle by granting access to specific PHI datasets, clinical applications, and administrative functions based on the minimum access required for each user's documented clinical or operational role. Privileged access management (PAM) governs the subset of highly sensitive access actions including database administrator sessions, security configuration changes, and bulk PHI export operations through session recording, just-in-time privilege elevation, and automatic session termination on anomaly detection. Federated identity management integrates the health system's identity provider with cloud service providers, partner organizations, and telehealth platforms through industry-standard protocols (SAML 2.0, OpenID Connect, SMART on FHIR), enabling cross-organizational care coordination without creating shared credential stores that would violate ZTA's trust minimization principle.

Layer 3: Network Micro-Segmentation

The micro-segmentation layer implements ZTA's "assume breach" principle by designing the network architecture to limit the blast radius of any successful intrusion. The UZTHF recommends a software-defined perimeter (SDP) architecture that replaces traditional VPN and network perimeter controls with identity-verified, encrypted, per-session tunnels that grant access only to the specific application resource required not the broader network segment. This approach directly addresses the lateral movement vulnerability that enabled the propagation of ransomware in multiple high-profile healthcare incidents. For cloud-native workloads, service mesh technologies (Istio, Linkerd) enforce mTLS between microservices and apply traffic policies based on service identity certificates, ensuring that even intra-cluster communication follows ZTA verification principles. Dedicated PHI data flow policies govern the specific pathways through which ePHI may traverse the cloud environment, prohibiting PHI transmission through any pathway not explicitly authorized in the policy engine a direct implementation of HIPAA's minimum-necessary standard.

Layer 4: Data Security and PHI Protection

The data security layer operationalizes HIPAA's technical safeguard requirements (§ 164.312) through encryption, data loss prevention, and information governance controls. All PHI stored within the UZTHF environment is encrypted using AES-256 with cloud-provider-managed or customer-managed encryption keys stored in FIPS 140-3 validated hardware security modules. PHI in transit including FHIR API payloads, HL7 messages, DICOM image transfers, and telehealth video streams is encrypted using TLS 1.3 as the minimum acceptable protocol, with TLS 1.0 and 1.1 explicitly prohibited. Data

classification policies automatically tag PHI datasets according to their sensitivity level (PHI, de-identified, aggregated), triggering graduated access controls and DLP policies proportionate to the data's sensitivity. Immutable audit logs stored in a write-once, read-many (WORM) configuration cryptographically linked to the blockchain-style hash chain provide tamper-evident records of all PHI access events, supporting both HIPAA audit control requirements (§ 164.312(b)) and forensic investigation of potential breaches.

Layer 5: Monitoring, Analytics and Response

The monitoring and response layer implements ZTA's requirement for continuous telemetry collection and real-time trust re-evaluation across all users, devices, and workloads in the healthcare cloud environment. A cloud-native SIEM platform integrated with UEBA, EDR, network detection and response (NDR), and cloud security posture management (CSPM) tools aggregates telemetry from all UZTHF layers into a unified security data lake. AI-driven behavioral analytics continuously model baseline behavior for each user identity and device, generating anomaly scores that feed the PDP's trust algorithm and trigger step-up authentication or access revocation when anomalous patterns are detected. Security Orchestration, Automation, and Response (SOAR) playbooks automate the initial containment and investigation steps for high-confidence threat detections including automatic account suspension on insider threat indicators, segment isolation on ransomware behavioral signatures, and HIPAA breach notification workflow initiation on PHI exfiltration detection reducing mean time to respond (MTTR) to the sub-hour timeframes documented in the highest-performing case studies.

Continuous Improvement Loop

The UZTHF's continuous improvement loop differentiates it from static compliance frameworks by embedding ZTA maturity progression as an organizational discipline. Annual red-team exercises, conducted by external adversarial simulation teams using healthcare-specific MITRE ATT&CK scenarios, provide empirical measurement of residual ZTA gaps. Threat intelligence integration through Health-ISAC membership feeds real-time IOCs and TTPs from healthcare-sector incidents into the UZTHF policy engine, enabling preventive control updates ahead of threat actor campaigns. Framework versioning aligned with NIST SP 800-207 updates, HHS OCR guidance revisions, and emerging cloud service provider security capability releases ensures that the UZTHF remains current without requiring complete architectural redesign. Workforce development programs, structured around the NICE Cybersecurity Workforce Framework and healthcare-specific competency models, address the talent gap identified as a primary adoption barrier.

Table 5. Proposed Zero-Trust Architecture Framework for US Cloud Healthcare – Core Components and Metrics

Framework Layer	Key Components	Implementation Mechanisms	Success Metrics
Governance & Compliance	HIPAA/HITECH alignment, board oversight, vendor risk management, policy lifecycle	ZTA policy engine mapped to NIST SP 800-207; quarterly HIPAA risk assessments; SBOM registry	Regulatory finding rate; vendor risk score; policy coverage index
Identity & Access Management	MFA, RBAC/ABAC, federated identity, just-in-time (JIT) privilege, PAM	Azure AD / Okta integration; CyberArk PAM; SAML/OIDC federation; biometric step-up auth	MFA adoption %; JIT session rate; privileged account anomaly rate
Network Micro-Segmentation	Software-defined perimeter, encrypted inter-service	Istio service mesh; Illumio / Guardicore micro-	Lateral movement incidents; east-west encrypted traffic %;

	mesh, SDN controls, VLAN isolation	segmentation; AWS VPC segmentation; mTLS	segment breach containment time
Data Security & PHI Protection	AES-256 encryption at rest/transit, DLP, tokenization, data classification, backup integrity	Microsoft Purview / Macie; Thales CipherTrust; FHIR-secured APIs; immutable audit logs	PHI exposure incidents; DLP policy trigger rate; encryption coverage %; backup restore success rate
Monitoring, Analytics & Response	SIEM, UEBA, AI behavioral analytics, automated playbooks, real-time alerting	Splunk / Chronicle SIEM; Darktrace UEBA; SOAR playbooks; 24/7 SOC integration; MITRE ATT&CK mapping	MTTD; MTTR; false positive rate; SOC alert-to-action time; ATT&CK coverage score
Continuous Improvement	Red-team exercises, threat intelligence sharing, framework versioning, workforce training	Annual penetration testing; H-ISAC threat feeds; tabletop exercises; ZTA maturity model assessments	Maturity level score; training completion %; red-team finding closure rate; framework update cadence

Discussion of Findings

The findings of this systematic review and the proposed UZTHF make several distinctive contributions to the fields of healthcare informatics, cybersecurity architecture, and regulatory compliance scholarship. At the empirical level, the consistency of positive security outcomes across the five case studies spanning diverse organizational scales, cloud platforms, and ZTA implementation approaches provides compelling evidence that ZTA is not merely a theoretical construct but a practically achievable and measurably beneficial security architecture for US healthcare cloud environments. The weighted mean improvements across cases 74% reduction in unauthorized access incidents, 68% reduction in breach detection time, and an average HIPAA audit finding reduction of 62% substantially exceed the outcomes documented for prior-generation perimeter-based security implementations.

Addressing the Research Questions

RQ1 asked how effectively current federal frameworks align with cloud-based healthcare security requirements. The analysis confirms that NIST SP 800-207 provides a technically comprehensive ZTA reference architecture well-suited to cloud-native healthcare deployments, but requires supplementation with HIPAA-specific implementation mappings and FedRAMP controls to satisfy the full regulatory obligations of covered entities. The UZTHF's governance layer addresses this gap by providing explicit crosswalks between ZTA technical controls and HIPAA Security Rule provisions, enabling healthcare compliance programs to treat ZTA implementation as a primary vehicle for HIPAA risk management.

RQ2 asked about primary threats and ZTA mitigations. The threat taxonomy presented in Table 1 and elaborated through the thematic analysis demonstrates that ZTA's design specifically its continuous identity verification, micro-segmentation, and behavioral analytics capabilities structurally addresses the seven most prevalent threat categories facing healthcare cloud environments. Notably, ZTA's assumed-breach posture means that even successful initial compromises are contained before they can escalate to the large-scale PHI exfiltration events that generate HIPAA breach notification obligations and HHS OCR enforcement actions.

RQ3 asked about implementation barriers and mitigation strategies. The adoption barrier analysis (Figure 5) and case study evidence collectively indicate that phased implementation prioritizing IAM and monitoring as the highest-impact, most technically

accessible ZTA components before advancing to micro-segmentation and full data security layer deployment is the most effective strategy for healthcare organizations with constrained resources and complex legacy environments. The UZTHF's modular layer design was explicitly informed by this finding, enabling incremental adoption without requiring organizations to achieve comprehensive ZTA maturity before realizing security benefits.

RQ4 asked about a unified HIPAA-aligned framework design. The UZTHF addresses this need by integrating five technical layers within a governance envelope that maps each layer's implementation actions to specific HIPAA Security Rule provisions, FedRAMP controls, and NIST CSF 2.0 functions. This integrated design enables healthcare CISOs to present ZTA implementation progress simultaneously as a cybersecurity maturity improvement and a regulatory compliance achievement, addressing the dual accountability structure technical security and legal compliance that characterizes healthcare information security governance.

Policy Implications

The findings carry several important policy implications for federal agencies and the healthcare industry. The HHS Office for Civil Rights should consider issuing ZTA-specific HIPAA implementation guidance that provides healthcare organizations with explicit mappings between NIST SP 800-207 components and HIPAA Security Rule technical safeguard provisions. Such guidance would reduce the interpretive burden currently placed on healthcare organizations and promote more consistent security implementations across the sector. The Cybersecurity and Infrastructure Security Agency (CISA), which has published sector-specific cybersecurity performance goals for healthcare, should update these goals to include ZTA adoption milestones that reflect the outcome evidence documented in this research.

Federal funding mechanisms including HHS's Health Care Cybersecurity Grant Programs and the Bipartisan Infrastructure Law's state cybersecurity grants should explicitly prioritize ZTA implementation assistance for critical access hospitals and rural health systems that lack the internal resources to implement ZTA independently. The case evidence demonstrates that the security benefits of ZTA scale with organizational size: smaller organizations with lower baseline security maturity may realize proportionally greater gains from ZTA adoption, provided they receive appropriate implementation support.

Theoretical Contributions

Theoretically, this study makes three contributions. First, it proposes the UZTHF as a novel theoretical construct the "healthcare cloud ZTA integration model" that operationalizes the intersection of ZTA architecture, HIPAA compliance, and cloud-native security design in a unified, empirically grounded framework. Second, it advances healthcare information security theory by demonstrating that regulatory compliance and security effectiveness are complementary rather than competing objectives in ZTA design: HIPAA's access control, audit control, and transmission security requirements align structurally with ZTA's verification, monitoring, and encryption pillars. Third, it contributes to the broader information systems security literature by providing an empirically validated case for paradigmatic security architecture transition in a regulated, safety-critical industry, complementing existing ZTA research conducted primarily in financial services and government contexts.

Conclusion

This study has investigated the design and implementation of Zero-Trust Architecture for securing cloud-based healthcare systems in the United States through a rigorous systematic literature review of 60 peer-reviewed studies, government standards, and validated case analyses, supplemented by evidence from five major US healthcare ZTA implementations. The resulting Unified Zero-Trust Healthcare Framework (UZTHF) provides a five-layer, HIPAA-aligned, cloud-native implementation architecture that addresses the full spectrum of security threats facing US healthcare cloud environments while providing a structured pathway to regulatory compliance.

The evidence base is unambiguous: ZTA consistently and substantially improves security outcomes in healthcare cloud environments, reducing unauthorized PHI access, accelerating breach detection, containing

ransomware propagation, and improving HIPAA audit performance across diverse organizational contexts. The architectural principle of continuous verification replacing implicit network trust with explicit, contextual, continuously re-evaluated access decisions directly addresses the structural vulnerabilities that have made US healthcare the most costly sector for cybersecurity breaches for thirteen consecutive years. However, the path to comprehensive ZTA adoption in US healthcare is neither simple nor uniform. Implementation complexity, legacy EHR integration, workforce skill gaps, and regulatory ambiguity represent genuine and substantial barriers, particularly for the majority of US hospitals that lack the scale and resources of the academic medical centers and integrated delivery networks documented in the case evidence. Addressing these barriers requires coordinated action from federal agencies (HHS OCR, CISA, NIST), cloud service providers, EHR vendors, and healthcare industry organizations a policy ecosystem response proportionate to the criticality of the infrastructure being protected.

Future research should prioritize three directions. First, longitudinal outcome studies tracking UZTHF-implementing organizations over multi-year periods will be essential for validating the framework's long-term security and compliance performance. Second, adaptation studies examining UZTHF applicability in resource-constrained settings including critical access hospitals, federally qualified health centers, and rural health clinics will extend the framework's reach across the full spectrum of US healthcare organizations. Third, investigation of emerging technology integrations particularly quantum-resistant cryptography, AI-driven policy engines, and blockchain-based PHI audit trails will ensure the UZTHF's relevance as the technology landscape continues to evolve.

Limitations

This study carries several limitations that contextualize its findings. The restriction to English-language publications may exclude relevant ZTA healthcare research from non-Anglophone healthcare systems in Europe and Asia, where advanced implementations have been documented in local-language literature. The case study evidence, while diverse, overrepresents large, technically sophisticated health systems with dedicated information security programs; the generalizability of the UZTHF to smaller organizations with limited security infrastructure has not been empirically tested. The absence of primary data collection survey instruments or structured interviews with healthcare CISOs and cloud architects limits the study's capture of unpublished implementation knowledge. Finally, the ZTA and healthcare cloud security landscapes evolve rapidly; specific technical recommendations regarding platforms, protocols, and regulatory requirements may require revision as new vulnerabilities, standards, and capabilities emerge.

REFERENCES

[1] Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: A survey. *Journal of Healthcare Engineering, 2019*, 1–15. Wiley

[2] Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2019). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 19*(1), 146.

[3] Balasubramanian, V., Stranieri, A., & Ramsay, H. (2021). Security vulnerabilities and challenges in cloud-based healthcare: A systematic review. *Future Internet, 13*(9), 231.

[4] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. Taylor & Francis

[5] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. IEEE

[6] Center for Internet Security. (2021). *CIS controls version 8.* Center for Internet Security

[7] Coventry, L., & Branley-Bell, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward. *Maturitas, 113*, 48–52. ScienceDirect

[8] Denyer, D., & Tranfield, D. (2009). Producing a systematic review. In D. A. Buchanan & A. Bryman (Eds.), *The SAGE handbook of organizational research methods* (pp. 671–689). SAGE.

[9] Executive Order 14028. (2021, May 12). Improving the nation's cybersecurity. *Federal Register, 86*(93), 26633–26649. Federal Register

[10] Ferrag, M. A., Maglaras, L., Janicke, H., Jiang, J., & Shu, L. (2023). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 76*, 103528.

[11] Fu, K., & Blum, J. (2013). Controlling for cybersecurity risks of medical device software. *Communications of the ACM, 56*(10), 35–37. ACM

[12] Grispos, G., Glisson, W. B., & Storer, T. (2021). Healthcare cybersecurity incidents and investigation: Exploring nurse practitioner perceptions. In *Proceedings of the 54th Hawaii International Conference on System Sciences (HICSS).* HICSS

[13] Hassan, W., Holt, T., & Ngo, F. (2023). A survey of zero-trust security practices in US health systems. *Journal of Cybersecurity and Privacy, 3*(2), 180–201.

[14] Health Information and Management Systems Society. (2023). *2023 HIMSS healthcare cybersecurity survey.* HIMSS. HIMSS

[15] Health-ISAC. (2023). *Health sector cybersecurity coordination center (HC3) 2023 annual threat report.* Health-ISAC / HHS. HHS

[16] HHS Office for Civil Rights. (2023). *Cybersecurity guidance: Recognized security practices and the HIPAA security rule.* US Department of Health and Human Services. HHS

[17] HHS Office for Civil Rights. (2024). *HIPAA breach notification rule: 2023 annual data breach summary.* US Department of Health and Human Services. HHS

[18] IBM Security. (2023). *Cost of a data breach report 2023.* IBM Corporation. IBM

[19] Kindervag, J. (2010). *No more chewy centers: Introducing the zero trust model of information security.* Forrester Research. Palo Alto Networks

[20] Lame, G. (2019). Systematic literature reviews: An introduction. In *Proceedings of the Design Society: International Conference on Engineering Design (ICED), 1*(1), 1633–1642. Cambridge

[21] Lizotte, D. J., Simmonds, M., Kanji, S., & Holbrook, A. M. (2020). Convergent integrated synthesis in systematic reviews: A practical guide. *Systematic Reviews, 9*(1), 256. Springer

[22] Mandel, J. C., Kreda, D. A., Mandl, K. D., Kohane, I. S., & Ramoni, R. B. (2016). SMART on FHIR: A standards-based, interoperable apps platform for electronic health records. *Journal of the American Medical Informatics Association, 23*(5), 899–908. PubMed

[23] Mehraj, S., & Banday, M. T. (2020). Establishing a zero trust strategy in cloud computing environment. In *2020 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1–6). IEEE. IEEE

[24] National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework 2.0 (NIST CSWP 29).* US Department of Commerce. NIST

[25] Oughton, E., Usher, W., Tyler, P., & Hall, J. (2022). Infrastructure as a complex adaptive system. *Complexity, 2022*, 1–17.

[26] Oyedeji, M. A., & Isaiah, I. A. (2026). Investigating the role of blockchain technology in enhancing supply chain security for US manufacturing industries. *International Journal of Modern Science and Research Technology, 4*(8), 581–596. Zenodo

[27] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. BMJ

[28] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture (NIST SP 800-207).* National Institute of Standards and Technology. NIST

[29] Rushanan, M., Rubin, A. D., Kune, D. F., & Swanson, C. M. (2014). SoK: Security and privacy in implantable medical devices and body area networks. In *2014 IEEE Symposium on Security and Privacy (SP)* (pp. 524–539). IEEE. IEEE

[30] Saracino, A., Sgandurra, D., Dini, G., & Martinelli, F. (2016). Madam: Effective and efficient behavior-based Android malware detection and prevention. *IEEE Transactions on Dependable and Secure Computing, 15*(1), 83–97. IEEE

[31] Securities and Exchange Commission. (2023). *Cybersecurity risk management, strategy, governance, and incident disclosure (Final Rule).* 17 CFR Parts 229 and 249. SEC

[32] Sousa, P. R., Resende, J. S., Martins, R., & Antunes, L. (2021). Scalable access control for multi-tenant cloud-native applications. In *Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES)* (pp. 1–9). ACM.

[33] Stafford, T. F. (2020). Zero trust networks. *Communications of the ACM, 63*(10), 19–21.

[34] Stanton, B., Greene, K. K., & Theofanos, M. (2022). Healthcare workers and cybersecurity: A survey of authentication practices. *Journal of Cybersecurity, 8*(1), tyac004.

[35] Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access, 10*, 57143–57179. IEEE

[36] Thati, V., & Sheltami, T. (2022). An intelligent approach for detecting healthcare cloud security threats using user and entity behavior analytics. *Computers & Security, 120*, 102807.

[37] Thomason, J. (2022). Digital health and cybersecurity in the age of COVID-19. *Frontiers in Digital Health, 4*, 874416. Frontiers

[38] Verizon. (2023). *2023 data breach investigations report.* Verizon Business. Verizon

[39] Walker-Roberts, S., Hammoudeh, M., & Dehghantanha, A. (2018). A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. *IEEE Access, 6*, 25167–25177. IEEE

[40] Ward, B., & Beyer, B. (2014). BeyondCorp: A new approach to enterprise security. *;login: USENIX Magazine, 39*(6), 6–11. USENIX