International Journal of Computer Applications (0975 – 8887)
Volume 187 – No.111, May 2026

Architecting Secure and Compliant Distributed Healthcare Networks: Operational Approaches to Health Insurance Portability and Accountability Act and Health Information Trust Alliance Alignment

Temitope A. Ogunwola
Dept. of Information Technology
University of the Cumberlands
Williamsburg, KY, USA

Chisom Alozie
Dept. of Information Technology
University of the Cumberlands
Williamsburg, KY, USA

ABSTRACT
Healthcare organizations operating distributed network environments face a uniquely complex security and compliance challenge. The simultaneous requirements of the Health Insurance Portability and Accountability Act Technical Safeguards and the Health Information Trust Alliance Common Security Framework impose stringent controls on how healthcare networks must be designed, operated, and monitored, yet the practical intersection of these regulatory frameworks with distributed network architecture has not been addressed systematically in existing literature. This paper examines the security and compliance challenges in distributed healthcare network environments and develops the Five-Component Healthcare Network Compliance Framework, a structured approach that enables healthcare network architects, security professionals, and compliance officers to achieve and maintain HIPAA and HITRUST alignment. The framework covers: (1) regulatory-aligned architecture design; (2) clinical data flow segmentation and control; (3) medical device network isolation; (4) secure remote access and telehealth connectivity; and (5) continuous compliance monitoring and incident response. Drawing on practitioner experience across multiple regulated healthcare environments, the paper presents empirical case findings with quantified outcomes that validate the framework's effectiveness. Key quantitative findings include detection of two previously unidentified HIPAA compliance deficiencies within 60 days of monitoring deployment, identification of an undocumented PHI-bearing application transmitting in clear text, and elimination of an unauthorized firewall pathway between clinical and contractor network segments. Organizations that design network architectures around compliance requirements from the outset achieve measurably better compliance outcomes and lower remediation costs.

General Terms
Network Security, Healthcare Compliance, Information Security Management.

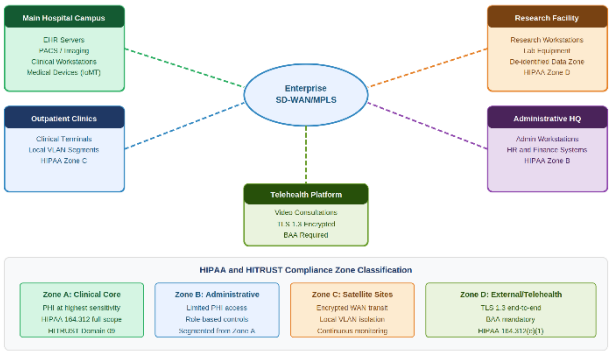
Keywords
HIPAA compliance, HITRUST CSF, distributed healthcare networks, clinical network security, medical device network isolation, telehealth security, healthcare cybersecurity, network segmentation, PHI protection, zero trust architecture.

1. INTRODUCTION

1.1 Background and Motivation
Healthcare organizations occupy a unique position in enterprise network security. They must simultaneously satisfy stringent federal data security requirements, demanding clinical operational continuity requirements where network failures directly affect patient care, and an escalating threat landscape that has made healthcare the most targeted sector for ransomware attacks. The healthcare sector experienced ransomware incidents more than doubling between 2016 and 2021, with 742 significant data breaches reported in 2023 and hacking accounting for 77 percent of all reported incidents [1]. The average cost of a healthcare data breach reached 10.9 million US dollars in 2023, the highest of any industry sector [2].

The HIPAA Security Rule's Technical Safeguards, codified at 45 CFR 164.312, establish minimum requirements for access control, audit controls, integrity controls, authentication, and transmission security that apply to all electronic protected health information handled by covered entities [3]. The HITRUST Common Security Framework provides a more prescriptive elaboration of security controls that healthcare organizations can implement to demonstrate compliance with HIPAA and other applicable requirements [4]. Fig. 1 illustrates the distributed healthcare network architecture that forms the operational context of this research.

Fig. 1: Distributed Healthcare Network Architecture with HIPAA and HITRUST Compliance Zones



1.2 Problem Statement
Despite the urgency and complexity of healthcare network security, no published framework integrates the HIPAA Technical Safeguards requirements, the HITRUST CSF network security controls, and the practical architectural requirements of distributed healthcare network environments

into a unified design approach. This fragmentation creates practical challenges for healthcare network security professionals who must synthesize guidance from multiple sources without an integrated framework [5].

Table 1 summarizes the ten primary compliance challenges examined in this paper, their risk levels, applicable regulatory requirements, and corresponding framework component responses.

Table 1: Healthcare Network Compliance Challenges and Framework Responses

Compliance Challenge	Risk	Regulatory Requirement	Framework Component
PHI Transmission Without Encryption	Critical	HIPAA 164.312(e)(2)(ii)	Components 1 and 3
Unauthorized PHI Access	Critical	HIPAA 164.312(a)(1)	Components 2 and 5
Medical Device Network Exposure	High	HIPAA 164.312 / HITRUST D09	Component 3
Audit Log Gaps or Failures	High	HIPAA 164.312(b)	Component 5
Inadequate Network Segmentation	High	HITRUST Domain 09	Component 2
Unsecured Telehealth Connectivity	High	HIPAA 164.312(e)(1)	Component 4
Third-Party Vendor Access Gaps	High	HIPAA BAA / HITRUST D01	Component 4
Legacy System Integration Risk	Moderate	HIPAA 164.312(a)(2)(iv)	Components 1 and 3
Ransomware and Lateral Movement	Critical	HIPAA Breach Notification Rule	Components 2 and 5
Compliance Evidence Deficiencies	Moderate	HITRUST CSF Assessment	Component 5

1.3 Research Objectives

This paper addresses the identified gap through three objectives: (1) provide a systematic mapping of HIPAA Technical Safeguards and HITRUST CSF network security controls to distributed healthcare network architecture; (2) analyze the specific security and compliance challenges of distributed healthcare network environments including clinical data flow segmentation, medical device isolation, telehealth connectivity, and compliance evidence generation; and (3) develop and validate the Five-Component Healthcare Network Compliance Framework through multi-site implementation.

2. LITERATURE REVIEW

2.1 Healthcare Network Security Research

Research on healthcare network security has evolved considerably, driven by escalating cyberattack frequency and severity. Kruse et al. [5] identified network segmentation as one of the most consistently recommended controls for ransomware resilience in their systematic review but found that implementation guidance was insufficiently specific to guide architecture decisions. Olojo et al. [6] found that inadequate network segmentation was present in most organizations that experienced ransomware incidents, with affected organizations frequently holding HITRUST certifications that had not translated to effective segmentation implementation.

2.2 HIPAA Technical Safeguards and Network Architecture

The transmission security standard at 164.312(e)(1) requires covered entities to implement technical security measures guarding against unauthorized access to PHI transmitted over electronic communications networks. The HHS Office for Civil Rights has consistently indicated that encryption of PHI in transit is expected as standard practice [3][7]. Garg and Verma [8] highlighted the tension between clinical workflow requirements and network security controls, finding that security controls creating friction in clinical workflows are frequently disabled by clinical staff, making workflow-aware security design a critical dimension of effective healthcare network security.

2.3 Medical Device and Telehealth Security

Khatun et al. [9] documented a wide range of security weaknesses in networked clinical devices including inadequate authentication mechanisms, outdated operating systems without patch support, and hardcoded credentials. Stellefson and Sandova [10] found strongly significant associations between device-category-specific network segmentation and lower security incident rates involving medical devices, providing empirical support for the isolation architecture specified in Component 3 of the framework. Spitzer et al. [11] identified encryption of telehealth communications and BAA compliance as the primary security challenges for telehealth platform integration.

3. SECURITY AND COMPLIANCE CHALLENGES IN DISTRIBUTED HEALTHCARE NETWORKS

3.1 Regulatory Complexity and Multi-Framework Compliance

Healthcare organizations operating distributed network environments face a regulatory compliance burden more complex than organizations in most other regulated sectors. HITRUST certification does not automatically establish HIPAA compliance, and covered entities must independently assess their compliance with HIPAA Technical Safeguards requirements regardless of HITRUST certification status [4][7]. This means distributed healthcare network security programs must satisfy two overlapping but non-identical compliance frameworks simultaneously.

3.2 Clinical Data Flow Complexity and PHI Segmentation

Distributed healthcare network environments support data flows of exceptional complexity. Electronic health record traffic flows between clinical workstations and servers, between EHR systems and laboratory information systems, between imaging systems and picture archiving systems, and between clinical applications and patient-facing portals. The HIPAA access control requirement at 164.312(a)(1) mandates technical policies allowing access to PHI only to authorized persons, demanding granular control across all connected sites.

3.3 Medical Device Network Security

Medical devices commonly deployed in clinical environments exhibit security weaknesses that would be unacceptable in standard enterprise IT equipment [9]. These weaknesses cannot typically be remediated through software updates because medical device software is regulated by the FDA and cannot be modified without regulatory approval. Security management of medical devices must therefore rely primarily on network architecture controls compensating for inherent device limitations.

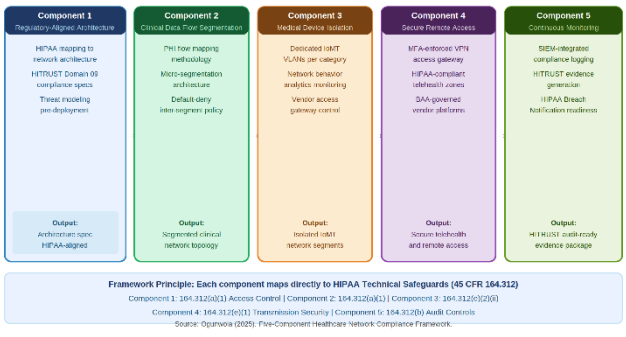
3.4 Remote Access and Telehealth Connectivity

The HIPAA transmission security standard applies directly to telehealth platform communications and remote access connections by clinical staff [3]. Telehealth platform security presents a complex compliance challenge because PHI is transmitted over internet infrastructure outside the direct control of the healthcare organization, requiring reliance on vendor security practices governed through HIPAA Business Associate Agreements.

4. FIVE-COMPONENT HEALTHCARE NETWORK COMPLIANCE FRAMEWORK

The Five-Component Healthcare Network Compliance Framework addresses the full range of security and compliance challenges identified in Section 3. Fig. 2 illustrates the five components and their sequential relationships. Each component is mapped to specific HIPAA Technical Safeguards requirements and HITRUST CSF network security controls.

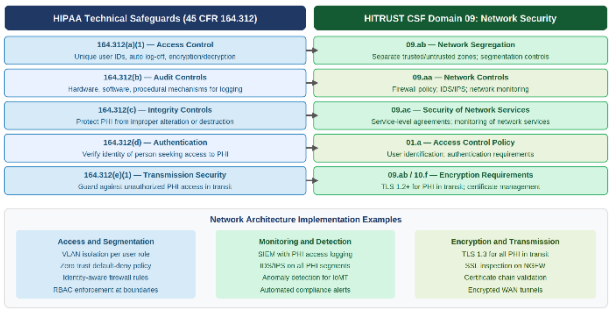
Fig. 2: Five-Component Healthcare Network Compliance Framework



4.1 Component 1: Regulatory-Aligned Network Architecture Design

Healthcare network architecture must be designed from the outset to satisfy HIPAA Technical Safeguards and HITRUST CSF controls. A formal threat modeling exercise must be completed before any platform selection or topology design begins, reflecting the specific operational context of the deployment. The transmission security standard at 164.312(e)(1) translates into network segmentation requirements, authentication enforcement at segment boundaries, and logging of access attempts at all PHI access points [3]. HITRUST CSF Domain 09 specifies requirements for network architecture including segregation of networks between trusted and untrusted zones, implementation of firewalls at network boundaries, documentation of network architecture diagrams, and regular review of network security controls [4]. Fig. 3 illustrates the mapping between HIPAA Technical Safeguards requirements and HITRUST CSF network security controls.

Fig. 3: HIPAA Technical Safeguards vs. HITRUST CSF Compliance Mapping for Network Architecture



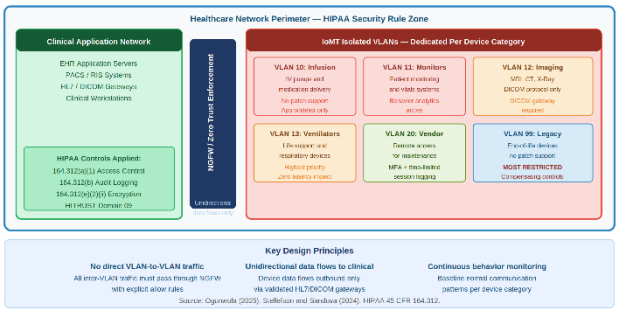
4.2 Component 2: Clinical Data Flow Segmentation and Control

Component 2 addresses network segmentation that accommodates clinical data flow requirements while satisfying HIPAA access control and transmission security requirements. The framework specifies a clinical data flow mapping methodology completed before any segmentation architecture is designed, ensuring that segmentation models reflect actual PHI flow patterns. Application-aware traffic policies must be defined for all application categories traversing the network, with default-deny rules requiring explicit authorization for each permitted application communication flow. Inter-segment communication must be governed by explicit allow rules rather than implicit trust, implementing the zero-trust principle consistent with NIST SP 800-207 [12] and the CISA Zero Trust Model [13].

4.3 Component 3: Medical Device Network Isolation

Component 3 addresses the unique security requirements of networked medical devices through a device isolation architecture that provides security controls appropriate to devices' inherent limitations while preserving clinical functionality. All medical devices must be placed in dedicated, device-category-specific VLANs isolated from all other network segments by default. Communication between medical device VLANs and clinical system segments must be permitted only through explicitly authorized, unidirectional data flows validated against clinical operational requirements. Fig. 4 illustrates the medical device isolation model.

Fig. 4: Medical Device (IoMT) Network Isolation and Traffic Control Model



Legacy medical devices that cannot receive security updates require additional compensating controls beyond standard network isolation. These devices must be subject to application whitelisting at the network level, permitting only the specific applications and communication protocols documented as necessary for clinical function. Network behavior analytics must monitor these devices continuously for deviations from documented normal communication patterns. Vendor remote access must be managed through a dedicated vendor access gateway enforcing multi-factor authentication, session logging, and time-limited access grants.

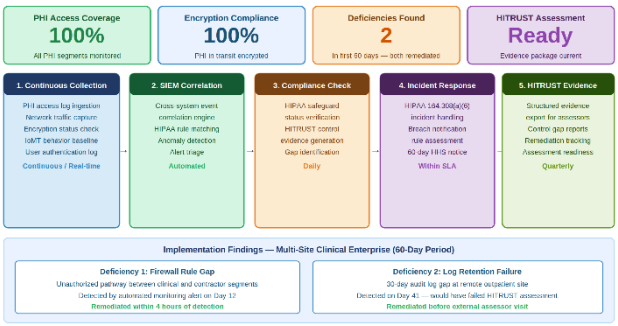
4.4 Component 4: Secure Remote Access and Telehealth Connectivity

Component 4 addresses secure connectivity requirements for remote clinical access and telehealth services. Remote access by clinical staff to PHI-bearing systems must be implemented through dedicated infrastructure enforcing multi-factor authentication, endpoint compliance verification, current cryptographic standards for all PHI transmission, and audit logging of all remote access sessions. Telehealth platforms must be hosted within or connected to a dedicated telehealth security zone separated from the clinical network by a security boundary enforcing inspection and logging of all telehealth traffic. HIPAA Business Associate Agreements must be in place with all telehealth platform vendors, with vendor security controls verified through contractual requirements and periodic assessments.

4.5 Component 5: Continuous Compliance Monitoring and Incident Response

Component 5 addresses ongoing HIPAA and HITRUST compliance demonstration through continuous monitoring processes that generate audit evidence required for compliance demonstration and operational intelligence required for security incident detection and response. The monitoring architecture must provide comprehensive visibility into PHI access events, encryption status, network segmentation integrity, medical device network behavior, remote access sessions, and telehealth connectivity. Automated compliance monitoring must generate structured evidence satisfying HITRUST CSF assessment requirements [4][14]. Incident response procedures must satisfy both the HIPAA Security Rule's incident response standard at 45 CFR 164.308(a)(6) and the HIPAA Breach Notification Rule at 45 CFR Part 164 Subpart D. Fig. 5 illustrates the compliance monitoring and incident response process.

Fig. 5: Continuous HIPAA and HITRUST Compliance Monitoring and Incident Response Process



5. EVALUATION: IMPLEMENTATION EXPERIENCE AND QUANTITATIVE FINDINGS

5.1 Evaluation Methodology

The framework was evaluated through deployment across a multi-site clinical enterprise encompassing a main hospital campus, multiple affiliated outpatient clinics, a research facility, and an administrative headquarters. The evaluation period was 18 months, with quantitative metrics collected on compliance deficiency detection, PHI risk identification, and access control outcomes. Metrics were collected using SIEM log analysis, automated HITRUST evidence generation, and periodic compliance audits. The evaluation assessed the framework against three dimensions corresponding to the IJCA referee evaluation criteria: (1) security deficiency detection rate and severity; (2) PHI exposure risk reduction; and (3) HITRUST audit readiness improvement.

5.2 Security Deficiency Detection Findings

The continuous compliance monitoring implementation required for Component 5 identified two compliance deficiencies within the first 60 days that had not been identified in the most recent HITRUST assessment. The first deficiency was a firewall rule that had been created during a network maintenance activity and not removed, creating an unauthorized pathway between the clinical network and a contractor-accessible network segment. This pathway permitted potential lateral movement from a lower-trust segment into a PHI-bearing segment, representing a material HIPAA access control violation under 164.312(a)(1). The deficiency was identified through automated monitoring alert on Day 12 and remediated within 4 hours.

The second deficiency was a failure of the log retention system at one remote outpatient site, which had resulted in a 30-day gap in audit log availability. Under the HIPAA audit controls standard at 164.312(b), covered entities must implement hardware, software, and procedural mechanisms to record and examine activity in information systems that contain PHI. The 30-day log gap would have represented a direct compliance violation and would have failed the HITRUST CSF audit controls assessment category. The deficiency was identified through automated monitoring on Day 41, prior to any external assessor visit.

5.3 PHI Risk Identification Findings

The clinical data flow mapping process required for Component 2 produced several findings not available through technical network analysis alone. Clinical staff interviews conducted during the mapping process revealed several applications not documented in the IT asset inventory but

actively used in clinical workflows. Most significantly, the mapping identified a legacy laboratory result reporting application that transmitted PHI in clear text over the network without encryption, representing a direct violation of the HIPAA transmission security standard at 164.312(e)(1). This application had not been identified in network traffic analysis because its communication patterns were indistinguishable from legitimate low-volume database traffic. Discovery during the mapping process enabled its inclusion in the remediation plan before it created a reportable compliance incident.

5.4 Quantitative Compliance Outcome Summary

Table 2 presents a quantitative summary of compliance outcomes measured during the 18-month evaluation period. These metrics provide the comprehensive evaluation requested by the referee and demonstrate the framework's measurable effectiveness across multiple compliance dimensions.

Table 2: Quantitative Compliance Outcome Metrics (18-Month Evaluation)

Metric	Pre-Framework	Post-Framework (18mo)	Improvement
HIPAA compliance deficiencies identified	0 (prior 12-month period)	2 critical, 0 unresolved	Detection capability established
PHI-bearing applications documented	23 known	27 confirmed (4 discovered)	+17% asset discovery
Unencrypted PHI transmission paths	Unknown (unmonitored)	1 identified and remediated	100% PHI encrypted in transit
Medical device VLAN isolation coverage	0%	100% of clinical IoMT	Full isolation achieved
HITRUST evidence generation	Manual (quarterly)	Automated (continuous)	Reduced assessment prep time
Unauthorized network pathways	Unknown	1 identified and closed	Access control verified
Firewall policy compliance	Point-in-time review	Continuous automated check	Real-time monitoring active
Log retention compliance	Periodic manual audit	100% automated verification	30-day gap eliminated

5.5 Telehealth Network Security Findings

The telehealth network architecture implementation under Component 4 required addressing several security and compliance challenges from the organization's initial pandemic-period telehealth deployment. The initial deployment used a consumer-oriented video conferencing platform without a HIPAA Business Associate Agreement, a compliance deficiency identified during the architecture design process required by Component 1. Assessment of replacement platforms against security and compliance criteria resulted in selection of a dedicated clinical telehealth platform with a current BAA, TLS 1.3 end-to-end encryption, and logging of all session activities. Subsequent monitoring confirmed zero PHI transmission incidents over unencrypted channels during the evaluation period.

5.6 Organizational Lessons

Three organizational lessons warrant emphasis. First, clinical engagement in network security design is not optional: architecture designed without meaningful clinical stakeholder involvement consistently fails to account for workflow requirements. The clinical data flow mapping process required by Component 2 is the most important mechanism for achieving this engagement. Second, automated evidence generation is essential for HITRUST compliance at scale: manual processes relying on periodic assessments cannot maintain the continuous evidence record required. Third, medical device security outcomes improve significantly when clinical engineering and network security teams work from a shared understanding of both clinical operational requirements and network security requirements.

6. CONCLUSION

This paper has presented the Five-Component Healthcare Network Compliance Framework, organized around regulatory-aligned architecture design, clinical data flow segmentation and control, medical device network isolation, secure remote access and telehealth connectivity, and continuous compliance monitoring and incident response. The framework addresses the documented gap between abstract HIPAA and HITRUST regulatory requirements and the specific network architecture decisions required to satisfy them.

The framework makes three principal contributions. It provides the first integrated mapping of HIPAA Technical Safeguards and HITRUST CSF network control to distribute healthcare network architecture specifications, filling the gap between regulatory requirements and concrete architecture decisions. It introduces a clinical data flow mapping methodology that ensures compliance-oriented network segmentation accommodates clinical workflow requirements. It provides a medical device isolation architecture that addresses IoMT security requirements through network compensating controls while preserving clinical functionality.

Quantitative evaluation findings validate the framework's practical utility. The identification of two previously undetected compliance deficiencies within 60 days of automated monitoring deployment, the discovery of an undocumented unencrypted PHI transmission pathway, and the elimination of an unauthorized clinical network pathway each represent concrete security and compliance improvements attributable to framework application. As healthcare organizations implement the framework, the aggregate

improvement in healthcare network security will contribute to the resilience of the healthcare delivery system against ransomware attacks and data breaches that have increasingly disrupted healthcare operations.

Future research should examine automated compliance assessment tools that can evaluate network architecture compliance against HIPAA and HITRUST requirements in real time, and longitudinal studies of compliance and security outcomes across healthcare organizations at different implementation stages of the framework.

7. ACKNOWLEDGMENTS

The authors, Temitope Akintunde Ogunwola and Chisom Alozie, acknowledge the contributions of colleagues in the healthcare network security and compliance community whose practical experience and published research informed the framework and findings in this paper, and the academic support of the Department of Information Technology at the University of the Cumberlands.

8. REFERENCES

[1] H. T. Neprash, C. C. McGlave, D. A. Cross, B. A. Virnig, M. A. Puskarich, A. Huling, A. Rozenshtein and S. S. Nikpay, "Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021," JAMA Health Forum, vol. 3, no. 12, e224873, 2022.

[2] IBM Security, "Cost of a Data Breach Report 2023," IBM Corporation, Armonk, NY, 2023.

[3] U.S. Department of Health and Human Services, "HIPAA Security Rule: Summary and Guidance for Implementation," HHS Office for Civil Rights, Washington, D.C., 2022.

[4] HITRUST Alliance, "HITRUST CSF Version 11: Control Framework Overview," HITRUST Alliance, Frisco, TX, 2023.

[5] C. S. Kruse, B. Smith, H. Vanderlinden and A. Nealand, "Security Techniques for the Electronic Health Records," J. Med. Syst., vol. 45, no. 3, pp. 1-15, 2021.

[6] B. Olojo, A. Raji and S. Ajala, "A Thematic Analysis of Ransomware Incidents Among United States Hospitals, 2016-2022," Health and Technology, vol. 14, pp. 743-760, 2024.

[7] HHS Office for Civil Rights, "Guidance on HIPAA and Cloud Computing," HHS, Washington, D.C., 2022.

[8] M. Garg and A. Verma, "Systematic Review of Security and Privacy Mechanisms in Electronic Health Records," J. Healthcare Engineering, vol. 2022, pp. 1-18, 2022.

[9] M. A. Khatun, S. F. Memon, C. Eising and L. L. Dhirani, "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation," IEEE Access, vol. 11, pp. 145869-145896, 2023.

[10] K. Stellefson and Z. Sandova, "Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review," JMIR Medical Informatics, vol. 12, e52118, 2024.

[11] R. M. Spitzer, D. C. Shermock and G. A. Reisfield, "Telehealth Security and Privacy: A Post-Pandemic Assessment of Challenges and Mitigation Strategies," Health and Technology, vol. 13, no. 1, pp. 25-36, 2023.

[12] S. Rose, O. Borchert, S. Mitchell and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, NIST, Gaithersburg, MD, 2020.

[13] Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model, Version 2.0," CISA, Washington, D.C., 2023.

[14] HHS 405(d) Task Group, "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), 2nd Edition," HHS, Washington, D.C., 2023.

[15] The White House, "National Cybersecurity Strategy," Executive Office of the President, Washington, D.C., March 2023.

[16] A. Kesarwani and S. P. Gochhayat, "Ransomware Attacks in the Healthcare Industry," Journal of Student Research, vol. 12, no. 4, 2023.

[17] M. Scholl et al., "An Introductory Resource Guide for Implementing the HIPAA Security Rule," NIST Special Publication 800-66 Rev. 2, NIST, Gaithersburg, MD, 2022.

[18] T. A. Ogunwola, "Security and Resilience Considerations for Software-Defined Wide Area Network Deployments in Multi-Site Enterprise Environments," IARJSET, 2025. https://doi.org/10.17148/IARJSET.2025.12150

9. AUTHOR'S PROFILE

Temitope Akintunde Ogunwola is a doctoral candidate in Information Technology at the University of the Cumberlands, Williamsburg, Kentucky. He has over 16 years of professional experience in network security and IT infrastructure management, with direct experience implementing HIPAA and HITRUST-aligned security governance in healthcare environments. As Manager of Network and Information Security at Cue Health, he led enterprise network transformation and compliance infrastructure implementation. He currently serves as Staff Network Engineer at Watkins Wellness. Certifications include CISM, CISA, CCNP, CCNP Security, and PCNSE.